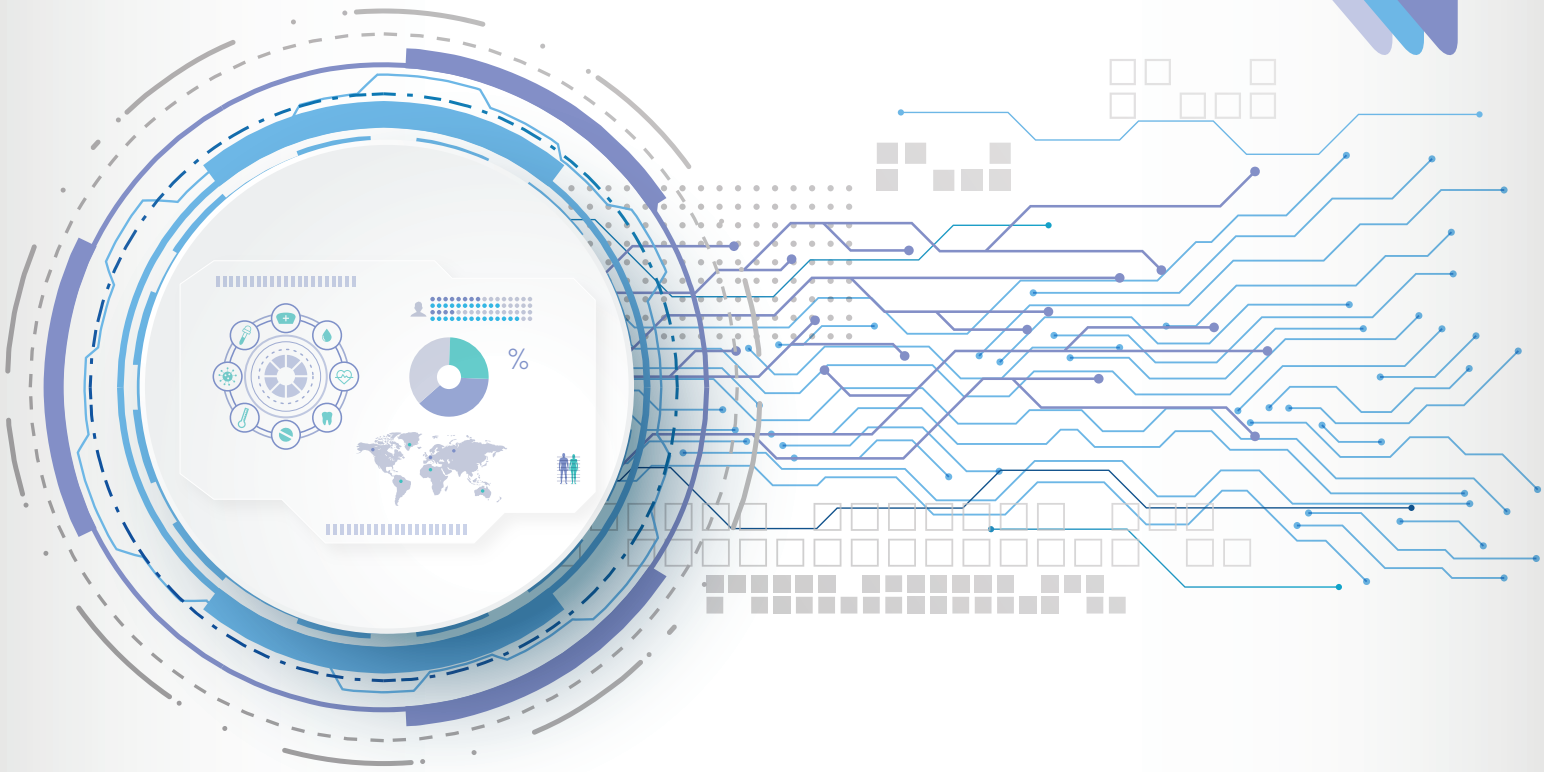
وزارة الصحـــــــــة

السياسة الوطنية لحوكمة وإدارة المعلومات الصحية

مايو ٢٠٢٤م

OmanHealth OmaniMOH
www.moh.gov.om 24441999



السياسة الوطنية لحوكمة وإدارة المعلومات الصحية

تمهيـــــد

تلعب المعلومات الصحية دورًا هامًا في دعم عجلة الاقتصاد العالمي، حيث تتسابق المؤسسات الصحية الحكومية والخاصة حول العالم لصنع قرارات مبنية ومستندة بشكل أساسي على المعلومات وذلك لما وجد من أثر هذه المنهجية الجوهري على نمو المؤسسات الصحية بشكل كبير وتجنب المخاطر المرتبطة بسير أعمالها. وقد أثبتت المعلومات في سيناريوهات عدة أنها سلاح ذو حدين من حيث النتائج والمخرجات، ففي حال تمت إدارتها بشكل صحيح ستؤدي القرارات المبنية عليها إلى نتائج جيدة، أما في حال الإدارة الخاطئة فستؤدي إلى نتائج غير مرغوب فيها، أي أن سر الاستفادة منها وجعلها أصل ذو قيمة يكمن في اتباع سياسات وضوابط مناسبة لحوكمة وإدارة المعلومات.

ومن هذا المنطلق قامت وزارة الصحة بإعداد السياسة الوطنية لحوكمة وإدارة المعلومات الصحية، وذلك تماشيا مع رؤية عُمان ٢٠٤٠، وخطى البرنامج الوطني للتحول الرقمي لتحقيق رؤية سلطنة عُمان المتعلقة بالتغطية الصحية الشاملة وأهداف التنمية المستدامة للصحة. ونظرا لأهمية الأمر وتأكيدا على ضرورة العمل المشترك والأخذ بوجهات النظر، فقد تم صياغة هذه السياسة بالتنسيق مع جميع الجهات ذات العلاقة بسلطنة عُمان.

ومع اتساع حجم المعلومات الصحية الرقمية، ستسهم هذه السياسة بشكل كبير في تحقيق التكامل المعلوماتي بين المؤسسات الصحية، تسهيل التبادل الآمن للمعلومات الصحية بين الأطراف ذات العلاقة، وحماية حقوق المرضى عند التعامل مع المعلومات الصحية الخاصة بهم. كما أن تطبيق هذه السياسة سيعمل بالتأكيد على تحسين جودة المعلومات الصحية مما سيعزز بدوره الجودة العامة لخدمات الرعاية الصحية، ويسهم في تنظيم إستخدام موارد الرعاية الصحية بالكفاءة والنوعية المطلوبة، ويساعد في إعادة تصميم وتقييم نماذج جديدة للخدمات الصحية، ويدعم تخطيط السياسات الصحية العامة وتقييمها، ويشجع الابتكار العلمي في المجال الصحي.

عليه، يتطلب من المؤسسات التي تعالج البيانات الصحية بسلطنة عُمان العمل بهذه السياسة بما في ذلك التدابير التكنولوجية والمادية والتنظيمية المصممة لحماية الخصوصية والأمن الرقمي، وتحقيق الشفافية حول أغراض معالجة البيانات الصحية، والحرص على تدريب معالجي البيانات الصحية وتطوير مهاراتهم بشكل مستمر. ولضمان الاستفادة القصوى من هذه السياسة تعمل وزارة الصحة على وضع آليات لرصد وتقييم أثرها بشكل دائم، سعيا منا بأن تصبح السياسة الوطنية لحوكمة وإدارة المعلومات الصحية بسلطنة عُمان مرجعا مثاليا يستفاد منه إقليميا ودوليا.

والله ولي التوفيق

الدكتور/ هلال بن علي بن هلال السبتي
وزير الصحة

المحتـــــــوى

المحتـــوى:

الفصـــــــل الأول

التعاريـــــف

التعاريف: يكون للكلمات والعبارات الآتية المعنى المبين قرين كل منها ما لم يقتض سياق النص معنى آخر.

1 ـ الوزارة: وزارة الصحة.

2 ـ المؤسسة الصحية: كل وحدة أو تنظيم مستقل للخدمات العلاجية والوقائية والتأهيلية والوقائية.

3 ـ الموظف: الأفراد العاملون بصفة مؤقتة أو دائمة، وكذلك المتدربون وموظفو الشركات المنفذين للمشاريع والمتطوعو الخاضعين لهذه السياسة. كما تشمل هذه السياسة أيضاً أي شخص يستخدم أنظمة المؤسسة.

4 ـ الحاسب الآلي: كل جهاز أو معدة تقنية قادرة على التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها سواء كانت تلك الأجهزة مكتبية أو محمولة أو لوحية وغيرها.

5 ـ البرنامج المعلوماتي: مجموعة من التعليمات والأوامر قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة محددة.

6 ـ النظام المعلوماتي: مجموعة من البرامج والأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

7 ـ الشبكة المعلوماتية: ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

8 ـ وسائط إلكترونية: وسيط مادي لحفظ وتداول البيانات والمعلومات الإلكترونية كالأقراص المدمجة والأقراص الضوئية والذاكرة الإلكترونية.

9 ـ الخوارزميات: سلسلة من التعليمات أو القواعد المحددة جيدا لحل فئة من المشكلات أو لإجراء العمليات الحسابية بواسطة أجهزة الحاسوب. حيث إن بعض هذه المشكلات أو العمليات الحسابية قد تحتاج إلى إختبار بعض الشروط والنظر إلى نتيجة الاختبار، إذا كانت النتيجة صحيحة تتبع مساراً يحوي تعليمات متسلسلة، وإذا كانت خاطئة تتبع مسار آخر مختلف من التعليمات.

10 ـ أنظمة الذكاء الاصطناعي: البرامج والتطبيقات الحاسوبية التي تحاكي القدرات الإدراكية البشرية وأنماط عملها من حيث القدرة على تحليل بيانات خارجية واستنباط قواعد معرفية جديدة منها، وحل المشكلات، والتعلم الذاتي، وتكييفها واستخدامها لتحقيق أهداف ومهام جديدة.

11 ـ أصول تقنية المعلومات: الحاسبات الآلية والنظم المعلوماتية والبرامج والشبكة وغيرها من الأجهزة والوسائط المستخدمة لإدارة ومعالجة المعلومات، وقواعد البيانات والمعلومات.

12 ـ البيانات: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات أيا كان شكله كالكتابة والحروف والأرقام والصور والأصوات والرموز والإشارات.

13 ـ رسالة بيانات إلكترونية: معلومات إلكترونية يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية كالبريد الإلكتروني أو البرق أو التلكس أو النسخ الورقي. بوسائل تقنية المعلومات.

14 ـ السجل الإلكتروني: العقد أو القيد أو رسالة المعلومات التي يتم إنشاؤها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو تسليمها بوسائل تقنية المعلومات على وسيط ملموس أو أي وسيط آخر قابل للتسليم بشكل يمكن فهمه.

15 ـ الموقع: مجال افتراضي له عنوان محدد على شبكة معلوماتية يهدف إلى إتاحة البيانات والمعلومات المعدة للعامة والخاصة.

16 ـ البريد الإلكتروني: وسيلة لتبادل رسائل إلكترونية، بين أكثر من شخص طبيعي أو اعتباري على عنوان محدد باستخدام وسائل تقنية المعلومات، عبر شبكة معلوماتية أو غيرها من وسائل الربط الإلكتروني بين وسائل تقنية المعلومات.

17 ـ الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.

18 ـ تبادل البيانات الإلكترونية: نقل المعلومات بين وسائل تقنية المعلومات باستخدام معيار متفق عليه لتكوين المعلومات.

19 ـ البيانات الشخصية: البيانات التي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة وذلك بالرجوع إلى معرف أو أكثر كالاسم أو الرقم المدني أو بيانات المعرفات الإلكترونيةأو البيانات المكانية أو بالرجوع إلى عامل أو أكثر خاص بالهوية الجينية أو الجسدية أو العقلية أو النفسية أو الاجتماعية أو الثقافية أو الاقتصادية.

20 ـ البيانات الجينية: البيانات الشخصية المتعلقة بالخصائص الموروثة أو المكتسبة جينيا والتي تنتج عن تحليل العينة البيولوجية.

21 ـ البيانات الحيوية: البيانات الشخصية التي تنتج عن معالجة فنية محددة تتعلق بالخصائص الجسدية أو النفسية أو السلوكية كصورة الوجه أو بيانات البصمة الوراثية.

22 ـ البيانات الصحية: البيانات الشخصية المتعلقة بالصحة الجسدية والعقلية والنفسية.

23 ـ المؤشرات الصحية: مجموعة من المعلومات الصحية تم جمعها ودراستها لوصف جانب معين من الصحة أو أداء النظام الصحي.

24 ـ إدارة المعلومات الصحية: مزيج من الممارسات بين إدارة الأعمال، والعلوم، وتكنولوجيا المعلومات تمكن القائم بها من تحليل وحفظ وحماية المعلومات الطبية الإلكترونية والورقية والحيوية بهدف توفير رعاية ذات جودة للمرضى.

25 ـ إخصائي إدارة المعلومات الصحية: موظف في المؤسسة الصحية يمثل حلقة الوصل بين شاغلي الوظائف الإكلينيكية، وشاغلي كل من: الوظائف التشغيلية، والإدارية، والمالية، يناط به اختصاصات استكمال، وحماية، وضمان توفر معلومات سريرية عالية الجودة، لأغراض مختلفة، منها: رعاية المرضى، والتعويضات، وضمان الجودة، والأبحاث، والإحصاءات، وصنع القرار، وضمان حصول المؤسسة الصحية على المعلومات المتاحة في أي وقت، مع الحفاظ على أعلى معايير سلامة البيانات والأمن والسرية.

26 ـ أدوات مراقبة الشبكة: الأجهزة والأدوات والبرمجيات المعدة لعمل تحليل فوري لحركة البيانات، وتوظيف المنطق المتقدم للكشف عن أنماط الأنشطة التي تشير إلى احتمالية وقوع هجوم إلكتروني على الشبكة أو التسلل إليها .

27 ـ الأمن السيبراني: حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من الهجمات الرقمية، من خلال تأمين البيانات والمعلومات التي يتم تداولها عبر الشبكات الداخلية أو الخارجية، وكذلك التي يتم تخزينها في خوادم داخل أو خارج المؤسسة من أي محاولات اختراق.

28 ـ أمن الشبكات: التدابير التي يتم اتخاذها لحماية مسار الاتصالات من الدخول غير المصرح به سواء العرضي أو المتعمد إلى العمليات العادية.

29 ـ الأمن المادي: حماية المنشآت والمعدات والمعلومات والبرمجيات وغيرها من السرقة والتخريب والكوارث الطبيعية أومن صنع الإنسان، والأضرار العرضية يا كانت أسبابها.

30 ـ أمن المعلومات: حماية البيانات ونظم المعلومات من الوصول، أو الاستخدام، أو الإفصاح أو التعطيل أو التعديل أو التدمير غير المصرح به عبر شبكة الإنترنت، وغير ذلك من المخاطر الداخلية أو الخارجية التي تهددها، وذلك من خلال توفير الأدوات والوسائل اللازمة لذلك.

31 ـ معالجة البيانات: عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية تتضمن جمعها أو تسجيلها أو تحليلها أو تنظيمها أو تخزينها أو أو تعديلها أو تحويرها أو استرجاعها أو مراجعتها أو تنسيقها أو ضم بعضها لبعض أو حجبها أو محوها أو إلغائها أو الإفصاح عنها عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى.

32 ـ التصريح: الموافقة، أو الترخيص، أو الإذن ، أو التفويض لشخص ما أو لشيء معين ليعمل عملاً محدداً ذي صلة.

33ـ إتاحة البيانات: كل وسيلة تحقق علم الغير بالبيانات الشخصية كالاطلاع والتداول والنشر والنقل والاستخدام والعرض والإرسال والاستقبال والإفصاح عنها.

34 ـ الاحتفاظ بالبيانات: تخزين السجلات الإلكترونية أو رسائل البريد الإلكتروني، المرسلة أو المستلمة، لفترة زمنية محددة، لغرض تلبية المتطلبات الإدارية والقانونية والمالية والتاريخية وغيرها.

35 ـ الأرشيف: وسائط إلكترونية معدة للتخزين طويل الأجل للمعلومات والبيانات - غالبا ما يكون على الشريط المغناطيسي- وذلك بغرض توفير إمكانية الحصول على نسخ احتياطية من السجلات النشطة، أو السجلات التي لم تعد في الاستخدام النشط.

36 ـ الاختراق: كل دخول غير مرخص به إلى بيانات شخصية أو وصول غير مشروع لها، أو أي عملية غير مشروعة لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول بهدف إلى الكشف أو الإفصاح عن البيانات الشخصية أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها.

37 ـ الإفشاء: كل ما من شأنه تمكين أو تسهيل اطلاع الغير على بيانات بخلاف أو تتجاوز المصرح لهم بالاطلاع عليها.

38 ـ انتهاك الخصوصية: الاطلاع على شؤون الآخرين دون علمهم أو إذن منهم، حتى ولو لم تكن أسرارا.

39 ـ البرامج الضارة: برامج يتم تصميمها لغرض إلحاق الضرر بالأنظمة والأجهزة، أو لسرقة معلومات حساسة من أجهزة الحاسب الآلي المستخدمة أو إبطاء تلك الأجهزة بالتدريج، أو إرسال رسائل بريد إلكتروني زائفة من حساب المستخدم دون علمه، وغير ذلك.

40 ـ البيانات الحكومية المفتوحة: البيانات المملوكة لوحدات الجهاز الإداري للدولة وغيرها من الأشخاص الاعتبارية العامة، والتي يمكن لأي شخص استخدامها، أو إعادة استخدامها، أو توزيعها مع مراعاة متطلبات ترخيص البيانات المفتوحة التي تُنشر بموجبها.

41 ـ البيئة الاختبارية: البيئة التجريبية المعزولة عن البيئة التشغيلية والتي يتم فيها اختبار أنظمة الذكاء الاصطناعي لفترات زمنية محددة للتأكد من خلوها من الأخطاء التقنية.

42 ـ البيئة التشغيلية: البيئة التي تم فيها تفعيل وتشغيل أحد إصدارات نظم الذكاء الاصطناعي واتاحته للمستخدمين.

43 ـ التحكم: قواعد وإجراءات، وسياسات قانونية وقائية تهدف إلى تقليل الانتهاكات، وذلك من خلال استخدام أجهزة أو أنظمة إلكترونية أو تقنية وغيرها.

44 ـ التحكم في الوصول: قواعد للحد من الوصول إلى أنظمة الحماية والبيانات في جميع الأوقات والظروف.

45 ـ التدقيق: جمع المعلومات عن أصول تقنية المعلومات والتحقق من صحتها وتحليلها لضمان الامتثال للقواعد واللوائح المعمول بها.

46 ـ التشفير: تحويل البيانات الإلكترونية من هيئتها كنصوص واضحة مقروءة إلى نصوص مشفرة غير مقروء بما يكفل إخفاء المعنى الأصلي لها للحيلولة دون معرفتها أو استخدامها.

47 ـ الرعاية الصحية عن بعد: مجال يتمّ فيه نقل المعلومات الطبيّة من خلال وسائط صوتيّة مرئيّة تشاركيّة بغرض الاستشارات الطبيّة والعمليّات الجراحيّة عن بعد أو التشخيص الطبيّ.

48 ـ التكامل : صيانة وضمان دقة واتساق البيانات.

49 ـ التلاعب: التغيير المتعمد لمنطق النظام، أو البيانات، أو معلومات التحكم، وذلك بغرض جعل النظام يؤدي وظائف أو خدمات غير مصرح بها.

50 ـ التوثيق النشط: توثيق البيانات الصحية في سجل الزيارة المفتوحة بالمؤسسة في حال فتح زيارة للمريض.

51 ـ التوثيق غير النشط: توثيق البيانات الصحية في السجل الصحي بالمؤسسة بإضافة ملحق بيانات إليه، وذلك في حال عدم فتح زيارة للمريض.

52 ـ الجدار الناري/ الحماية: جهاز أو برنامج يتولى مراقبة حركة البيانات عبر الشبكة، ويمكنه السماح للبيانات بالمرور أو رفض ذلك بحسب الإعدادات التي تم برمجتها فيه، ويعمل على تحسين حركة المرور في الشبكة، ويستخدم كذلك لأغراض أمنية.

53 ـ الحادث الأمني: حادث أو مجموعة حوادث ذات تأثير سلبي تهدد أمن أنظمة الحاسب والشبكات.

54 ـ الحوسبة السحابية: هي نموذج يتيح إمكانية الوصول في كل مكان وعند الطلب إلى مجموعة مشتركة من موارد الكمبيوتر القابلة للإعداد (مثل شبكات الكمبيوتر والخوادم ووحدات التخزين والتطبيقات والخدمات)، بسرعة وبأقل جهد إداري.

55 ـ الدعم الفني: المستوى الأول من تقديم الدعم للمستخدمين التقنيين ومستخدمي الشبكة. ويتضمن الدعم حل المشكلات وتلقي المكالمات ومساعدة مزودي الخدمات.

56 ـ الذكاء الاصطناعي في المجال الصحي: هو مصطلح عام يعبر عن استخدام خوارزميات التعلم الآلي وبرامجه (أي الذكاء الاصطناعي) لمحاكاة عمليات الإدراك البشري في تحليل البيانات الطبية والصحية المعقدة إضافةً لتقديمها وفهمها.

57 ـ السجل الصحي: السجل الذي يختص بجمع البيانات عن الفرد أو حالته الصحية من الولادة وحتى الوفاة.

58 ـ السجل الصحي الوطني: السجل الذي يختص بجمع البيانات عن الفرد أو حالته الصحية من الولادة وحتى الوفاة من خلال الربط مع المؤسسات الصحية ذات العلاقة بتقديم الخدمات الصحية للفرد.

59 ـ السجلات: هي المواد الوثائقية أو المعلومات، بصرف النظر عن الوسائط أو الخصائص المادية لها، التي يُنشئها أو يتلقاها المكتب فيما يتعلق بمعاملات الأعمال الرسمية والتي يحتفظ بها هذا المكتب كدليل على وظائف المؤسسة أو سياساتها أو قراراتها أو إجراءاتها أو عملياتها، أو بسبب قيمة البيانات الواردة في ذلك السجل.

60 ـ السرية: الحاجة إلى ضمان أن المعلومات لا يُفصح عنها إلا للمخول لهم بذلك.

61 ـ استشارة خبير عن بعد: هي استشارة طبية عن بعد بين الممارسين الصحيين للاطلاع على رأي طبي اخر تعتمد على تقنية تخزين وإعادة توجيه.

62 ـ التشخيص عن بعد: هي تقديم تشخيص عن بعد عن طريق ممارس صحي بدون اتصال متزامن مع المريض.

63 ـ المساعدة عن بعد: هي تقديم الدعم الطبي المتزامن عن بعد من قبل ممارس صحي وذلك لمساعدة ممارس صحي اخر من اجل القيام بإجراء طبي.

64 ـ الإشراف الطبي عن بعد: هي الإدارة الطبية الكاملة عن بعد للمرضى المنومين من قبل الممارس الصحي.

65 ـ الاستشارة عن بعد: هي استشارة عن بعد بين المريض والممارس الصحي.

66 ـ الضمانات الإدارية: الإجراءات والسياسات الإدارية، والإجراءات لإدارة اختيار وتطوير وتنفيذ وصيانة الإجراءات الأمنية لحماية المعلومات الصحية الإلكترونية المحمية وإدارة سلوك القوى العاملة في الكيان المشمول. فيما يتعلق بحماية تلك المعلومات.

67 ـ الضمانات الفنية: التكنولوجيا وإجراءات استخدام السياسات لحماية المعلومات الصحية الإلكترونية المحمية ولتحكم في الوصول إليها.

68 ـ الضمانات المادية: التدابير المادية والسياسات والإجراءات لحماية أنظمة المعلومات الإلكترونية للكيان المُغطى والمباني والمعدات ذات الصلة، من المخاطر الطبيعية والبيئية والتطفل غير المصرح به.

69 ـ القرارات المؤتمتة: العمليات الحاسوبية التي يتم فيها اتخاذ القرارات آلياً عن طريق التعلم الذاتي أو الإحصاءات أو الخوارزميات أو غيرها من تقنيـات معالجـة البيانات، دون أي تدخل بشري.

70 ـ القرارات غير المؤتمتة: العمليات الحاسوبية التي تحتاج الى مدخلات بشرية كالبيانات أو الأوامر التنفيذية لتتم فيها عمليات اتخاذ القرارات.

71 ـ الكوارث: أي حدث يجعل المؤسسة غير قادرة على توفير وظائف الأعمال الرئيسية لفترة زمنية. وقد يشمل

ذلك: أي حدوث أو تهديد وشيك بحدوث أضرار جسيمة أو خطيرة أو إصابات أو خسائر في الأرواح أو ممتلكات ناتجة عن حادث أمني طبيعي أو تكنولوجي أو وطني (مثل: الحرائق أو التخريب أو الكوارث الطبيعية أو فشل النظام).

72 ـ المتحكم: الشخص الذي يتولى تحديد أهداف ووسائل معالجة البيانات الشخصية، ويقوم بهذه المعالجة بنفسه، أو يعهد بها إلى غيره.

73 ـ المريض: هو أي فرد يتلقى العناية الطبية من قبل أي مزاول في الرعاية الصحية أو يتم قبوله في المنشأة الصحية.

74 ـ المستخدم: هو كيان ما، سواء كان شخصاً أو مؤسسة أو آلية مهيأة للوصول إلى نظام ما بإذن أو بدونه

75 ـ المعالج: الشخص الذي يقوم بمعالجة البيانات الشخصية نيابة عن المتحكم.

76 ـ المعالجة: عملية أو مجموعة عمليات يتم إجراؤها على البيانات، تتضمن جمعها أو تسجيلها أو تحليلها أو تنظيمها أو تخزينها أو تعديلها أو تحويرها أو استرجاعها أو مراجعتها أو تنسيقها أو ضم بعضها لبعض أو حجبها أو محوها أو إلغاءها أو الإفصاح عنها، عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى.

77 ـ المعلومات الحساسة: هي المعلومات المميزة أو الخاصة التي يُسمح لبعض الأشخاص فقط برؤيتها وبالتالي لا يمكن للجميع الوصول إليها. وهي المعلومات / البيانات التي ستكون غير ملائمة إذا ما أصبحت معروفة للآخرين (مثلا: المعلومات الصحية، أو السجل الجنائي).

78 ـ المعلومات السرية: جميع المعلومات غير المتاحة للجميع وإنما للمخول لهم فقط وفق الصلاحيات الممنوحة أوهي المعلومات التي يجب ألا تدخل في المجال العام، ويجب على الموظفين حمايتها من أي استخدام أو إفصاح غير مصرح به، لما فيه من احتمالية إيقاع ضرر بالفرد أو المؤسسة الصحية.

79 ـ المعلومات الصحية الإلكترونية المحمية: هي أي معلومات حول الحالة الصحية، أو توفير الرعاية الصحية، أو الدفع مقابل الرعاية الصحية التي يتم إنشاؤها أو جمعها بواسطة أحد مقدمي الرعاية الصحية إلكترونياً والتي تتطلب استخدام الأسس والقوانين المفروضة للأمن والخصوصية.

80 ـ المعلومات الصحية مجهولة الهوية: معلومات صحية من سجل طبي تم تجريده من جميع «المعرفات المباشرة» - أي جميع المعلومات التي يمكن استخدامها لتحديد المريض الذي تم اشتقاق المعلومات الصحية من سجله الطبي.

81 ـ المعلومات الصحية محددة الهوية للفرد: هي معلومات صحية يمكن ربطها بشخص معين أو إمكانية تحديد هوية الفرد من تلك المعلومات.

82 ـ المعلومات الصحية: هي البيانات المتعلقة بالتاريخ الطبي للشخص، بما في ذلك الأعراض، التشخيصات، الإجراءات، والنتائج. تتضمن سجلات المعلومات الصحية تاريخ المرض، نتائج المختبر، الأشعة، المعلومات السريرية، والملاحظات.

83 ـ المعلومات عالية السرية: هي المعلومات التي تعتبرها المؤسسة الصحية معلومات عالية الحساسية ومعلومات حساسة. والتي يجب أن يكون الوصول إليها مقيد بموجب القوانين والسياسات لعدد معين من الأشخاص المصرح لهم بذلك، ويمكن أن يؤدي سوء استخدامها إلى إيقاع ضرر كبير بالفرد أو المؤسسة الصحية.

84 ـ النص المقروء: النص العادي قبل أن يتم ترميزه إلى نص مشفر أو بعد فك تشفيره.

85 ـ الوصول: القدرة على قراءة أو كتابة أو تعديل أو نقل البيانات / المعلومات.

86 ـ الجراحة عن بعد: هي عملية جراحية او تدخل جراحي عن بعد يقوم به ممارس صحي للمريض.

87 ـ برامج مشتركة: برامج محمية بحقوق الطبع والنشر متوفرة على أساس تجريبي.

88 ـ برنامج الكشف عن الفيروسات: البرنامج الذي يعنى بالدفاع والتأمين وتحصين جهاز الحاسب الآلي ضد الفيروسات وغيرها من البرمجية الخبيثة. كما تعمل هذه البرامج على مسح المرفقات الواردة في البريد الإلكتروني وغيرها من البرامج للتأكد من سلامتها.

89 ـ بيانات الأعمال الهامة: البيانات التي يجب نسخها احتياطيا بشكل متكرر نظرًا لأهميتها لنظام تكنولوجيا المعلومات.

90 ـ ترخيص البرامج: اتفاقية قانونية بين المطور ومستخدم البرنامج الذي يحدد شروط توزيع هذا البرنامج وتخزينه واستخدامه.

91 ـ ترقية البرمجيات: عملية استبدال إصدار برنامج بإصدار أحدث من نفس البرنامج.

92 ـ تكنولوجيا المعلومات الصحية: هي تطبيق معالجة المعلومات التي تشمل كلاً من أجهزة الكمبيوتر والبرامج التي تتعامل مع تخزين واسترجاع ومشاركة واستخدام معلومات الرعاية الصحية والبيانات الصحية والمعارف للاتصال واتخاذ القرارات اللازمة.

93 ـ تقييم المخاطر: عملية تقييم تعرض أحد الأصول للتهديدات المحددة وفعالية الضمانات القائمة أو المقترحة لحماية الأصول.

94 ـ إدارة المخاطر: هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المؤسسة الصحية أو الشبكة المعلوماتية، والحد والتقليل من نقاط الضعف إن وجدت، للحد من المخاطر إلى مستوى مقبول.

95 ـ توافر المعلومات: إتاحة المعلومات الصحية الإلكترونية للاستخدام عند الطلب من قبل الشخص المصرح له.

96 ـ حادث أو تطفل: هو حدث ضار مرتبط بنظام معلومات يؤدي إلى فشل في الامتثال للوائح أو توجيهات الأمن الإلكتروني، نتيجة محاولة أو فقدان فعلي للبيانات يشمل إهدار الممتلكات أو المعلومات أو الاحتيال عليها أو إساءة استخدامها أو فقدها أو إتلافها عن طريق كشف / أو استغلال نقاط الضعف في الأجهزة أو البرامج.

97 ـ خادم ويب: جهاز رئيسي على الإنترنت يحمل مستندات ومعلومات وغيرها من الأمور المتعلقة بالتصفح على مستوى العالم ويجعلها متاحة للعرض بواسطة المتصفحات المختلفة.

98 ـ خطة التعافي من الكوارث: خطة تطبق على الأحداث الكبرى، التي عادة ما تكون كارثية، والتي تمنع الوصول إلى المنشأة الأساسية لفترة طويلة. تم تصميم هذه الخطة التي تركز على تقنية المعلومات لاستعادة إمكانية تشغيل النظام المستهدف أو التطبيق أو جهاز الحاسب الآلي في موقع بديل بعد حالة الطوارئ.

99 ـ سجل التدقيق: يلتقط إجراءات مستخدم الحاسب الآلي أثناء تسجيل الدخول إلى النظام ويحفظ المعلومات بجدول قاعدة بيانات أو ملف منسق.

100 ـ سرية المعلومات: عدم إتاحة المعلومات الصحية أو الكشف عنها للأشخاص غير المصرح لهم.

101 ـ سلامة المعلومات: عدم تغيير أو تدمير المعلومات الصحية بطريقة غير مصرح بها.

102 ـ شفرة ضارة: مصطلح يشمل رمز البرنامج أو البيانات التي يتم تضمينها أو إدراجها عن قصد في نظام معلومات لغرض غير مصرح به، دون علم المستخدم. تشمل الأمثلة الفيروسات والقنابل المنطقية.

103 ـ ضوابط الرقابة: استخدام الأجهزة أو البرامج أو الإجراءات لتسجيل وفحص نشاط النظام/الأنظمة.

104 ـ فك التشفير: عملية تحويل رسالة مشفرة إلى النص الأصلي المقروء.

105 ـ فيروس الحاسب الآلي: نوع من أنواع البرمجيات الخبيثة التي صنعت لأغراض تخريبية منها المدمرة للملفات سواءً ملفات النظام أو الملفات المكتبية وأخرى لتغيير الخصائص المتعلقة بتلك الملفات وتتكاثر عن طريق توليد نفسها من خلال الشفرات المصدرية لتلك الفيروسات أو عن طريق برامج خبيثة.

106 ـ كسر كلمة المرور: محاولة تخمين كلمة المرور من قبل شخص غير مصرح له تعمدا.

107 ـ كشف التسلل: نظام إدارة أمنية لأجهزة الحاسوب والشبكات. يجمع نظام كشف التسلل المعلومات من مختلف المناطق داخل الحاسوب أو شبكة الاتصال ويحللها، وذلك لتحديد الخروقات الأمنية المحتملة، بما يشمل الهجمات من خارج المؤسسة، أو إساءة الاستخدام من داخلها.

108 ـ مراقبة الشبكة: هو الكشف عن حالة الشبكة وسلامتها والحد من محاولات الانقطاع أو التطفل من خلال مراجعة السجلات أو غيرها من المعلومات المتاحة على الشبكة، ويعد كشف التسلل أمراً ضرورياً للحفاظ على أمن الشبكات.

109 ـ مرحلة التدمير: هي تلك الفترة التي اكتملت فيها الحاجة للسجل، وأكمل فيها السجل مرحلة الاحتفاظ والفترة الزمنية المحددة لذلك.

110 ـ مسح الفيروسات: عملية لفحص ترميز الحاسب الآلي / البرامج بالتتابع، جزء بجزء. بالنسبة للفيروسات، يتم إجراء عمليات مسح لتوقيعات الفيروسات أو الممارسات غير الآمنة المحتملة على سبيل المثال، التغييرات التي يتم إجراؤها على ملف قابل للتنفيذ، والكتابة المباشرة إلى قطاعات القرص المحددة.

111 ـ معالجة البيانات: هو علم يهتم بإعادة معالجة البيانات بحيث يمكن إدخالها في شكل بيانات محوسبة في شكل خوارزميات ولغات البرمجة

112 ـ مصادر المعلومات: مجموعة من المكونات اليدوية والآلية، كل منها يدير مجموعة بيانات محددة أو مصدر معلومات.

113 ـ ملفات النسخ الاحتياطي: إجراءات عمل نسخ احتياطية من الملفات الإلكترونية التي تم إنشاؤها بغرض حفظها من الضياع في حالة فقدان الملفات الرقمية الأصلية لأي سبب كان أو بغرض استعادتها إلى ما كانت عليه.

114 ـ موارد تقنية المعلومات: تشمل أجهزة الكمبيوتر، والخوادم، والمساعدين الرقميين الشخصيين، والطابعات، والآلات النسخ، والمحاور، والمبدلات، والموجهات، والجسور، ونقاط الوصول اللاسلكية، وبطاقات واجهة الشبكة أو الجدران النارية/ الحماية.

115 ـ نص التشفير: هو الرسالة التي بعثت في شكلها المشفر.

116 ـ نظام البريد الإلكتروني: هو برنامج أو وسيط يقوم بخدمة إرسال رسائل واستقبالها عبر أجهزة الحاسب الآلي من خلال الشبكات المحلية أو العالمية.

117 ـ نظم الإنذار المكتبية: نظم الإنذار التي تتعلق ببيئة العمل مثل إنذارات الحرائق وعدم وجود مواد خطرة بالمكتب وتتعلق بسلاسة ودقة البيانات المدخلة مثل تنبيهات عند إدخال بيانات غير صحيحة.

118 ـ مراقبة المريض عن بعد: هي مراقبة طبية عن بعد للمريض عن طريق ممارس صحي بناء على البيانات الطبية التي يتم جمعها ومشاركتها من قبل المريض او أحد مقدمي الرعاية الصحية.

119 ـ كسر الزجاج: يشير إلى إجراء يمكن المستخدم الذي لا يمتلك امتيازات الوصول للوصول إلى بيانات المرضى في حالات الطوارئ.

120 ـ شركاء العمل: الشركات التي تتعاقد معها المؤسسة الصحية لتقديم بعض الخدمات لها.

الفصـــــــل الثاني

١. المقدمـــة

٢. أهـــداف السياســـة

٣. نطـــاق التطبيـــق

٤. جهـــات الاختصـــاص

1 المقدمـــة :

تمثل المعلومات الصحية التي تنتجها المؤسسات الصحية الحكومية والخاصة عنصر أساسي في النظام الصحي وثروة وطنية يمكن الاعتماد عليها عند اتخاذ القرارات الاستراتيجية واستشراف المستقبل في عملية التخطيط. ونظرا لحجم المعلومات الصحية التي تصدر من كافه المؤسسات الصحية في سلطنة عمان وضمانا لجودتها ومحافظة على خصوصيتها وخصوصية أصحاب هذه المعلومات، ورفعا لسقف استخداماتها، اِتجهت وزارة الصحة بسلطنة عُمان بإعداد «السياسة الوطنية لحوكمة وإدارة المعلومات الصحية» للقطاع الصحي الحكومي والخاص لضمان تنفيذ المهام المناطة به بكفاءة وفاعلية.

تعد هذه السياسة بياناً رسمياً يجب الالتزام به أثناء إدارة المعلومات الصحية. كما أنها تضع إطارا يوضح الضوابط الواجب مراعاتها و تنفيذها داخل المؤسسة الصحية. في حين يمكن تحديد الإجراءات التفصيلية المناسبة لتنفيذ هذه السياسة في كل مؤسسة صحية بناء على طبيعة عملها ومستوى خدماتها.

ومن هذا المنطلق وتحقيقا للأهداف الاستراتيجية لرؤية عمان ٢٠٤٠، اتبعت وزارة الصحة منهجية واضحة أثناء إعدادها لهذه السياسة لضمان توفر المتطلبات والممارسات والمعايير المحلية والعالمية المتعلقة بمجال حوكمة وإدارة المعلومات والتي تتلخص في الآتي:

- أن تتناغم مع متطلبات وأهداف رؤية عمان ٢٠٤٠.
- ان تتوافق مع جميع المراسيم السلطانية ذات العلاقة.
- أن تتوافق مع لوائح وأنظمة وزارة الصحة.
- أن تتوافق مع استراتيجية عمان الرقمية ٢٠٣٠م، واستراتيجية التحول الرقمي وخطته التنفيذية ٢٠٢١-٢٠٢٥م.
- أن تتكامل مع سياسات وزارة النقل والاتصالات وتقنية المعلومات.
- أن تلتزم بتوجيهات وتوصيات مركز الدفاع الإلكتروني.
- أن تتوافق مع معايير المنظمات الدولية ذات العلاقة.

2 أهداف السياسة:

تهدف هذه السياسة إلى تحقيق الآتي:

1 - حماية خصوصية وأمن المعلومات الصحية.

2 - ضمان دقة جمع المعلومات الصحية، وتسجيلها، وتحليلها، وتنظيمها، وتخزينها، وتعديلها، وتحويرها، واسترجاعها، ومراجعتها، وتنسيقها، وضم بعضها لبعض، وحجبها، ومحوها، وإلغائها، والإفصاح عنها عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى.

3 - تعزيز مشاركة المسؤولين عن إدارة المعلومات الصحية في المؤسسات الصحية للقيام بدورهم في الإدارة الفعالة لدورة حياة المعلومة الصحية والإشراف على إدارة البيانات، والمحافظة على جودتها وسلامتها وتكاملها وخصوصيتها.

4 - تفعيل دور المسؤولين عن تقنية المعلومات في المؤسسات الصحية للقيام بدورهم في إدارة البنية التحتية التقنية والأجهزة والبرامج والتطبيقات التي تدعم العمل والاتصالات وقواعد البيانات التحليلية.

5 - تحديد الضوابط التي يجب اتباعها من قبل المؤسسات الصحية والعاملين فيها عند التعامل مع المعلومات الصحية.

6 - إرشاد وتوجيه المؤسسات الصحية والعاملين فيها إلى السياسات المتعلقة بالاستخدام الأمثل للبنية التحتية للشبكة المعلوماتية.

7 - حماية مصالح وتجهيزات المؤسسات الصحية من خلال قواعد واضحة ومحددة واجبة الاتباع عند تقديم خدماتها.

8 - توفير الأسس والأطر اللازمة لتنفيذ أعمال المراجعة الداخلية؛ لتقييم مدى الالتزام والتقيد بالأنظمة واللوائح والسياسات المتعلقة بخصوصية وأمن الشبكة المعلوماتية.

9 - تحديد آليات تطبيق اللوائح والقواعد والاستراتيجيات والتعليمات والتوصيات الصادرة من وحدات الجهاز الإداري للدولة المختصة داخل المؤسسات الصحية.

10 - تحقيق التكامل المعلوماتي بين المؤسسات الصحية.

11 - حماية حقوق المرضى عند التعامل مع المعلومات الصحية الخاصة بهم.

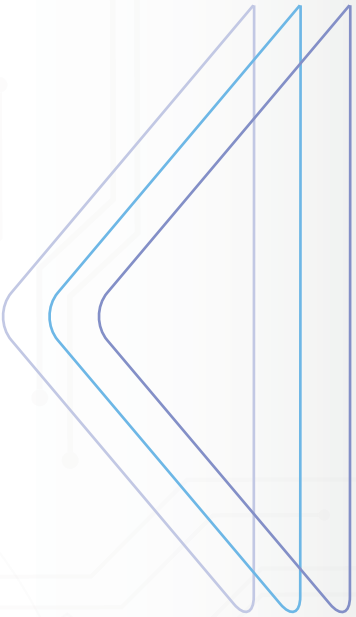
3 نطاق التطبيق:

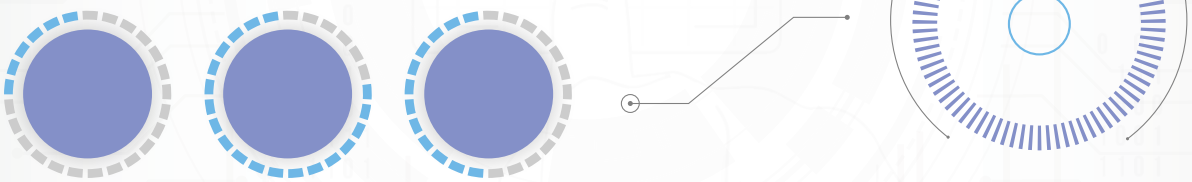
تسري أحكام هذه السياسة على المؤسسات الصحية الحكومية والخاصة بسلطنة عمان.

4 جهات الاختصاص:

1 - يجب على وزارة الصحة مراجعة وتحديث وتطوير أحكام هذه السياسة كلما اقتضت الحاجة، بعد التنسيق مع الجهات المختصة والجهات المعنية وفقا للقوانين والمراسيم السلطانية النافذة.

2 - لا تخل أحكام هذه السياسة بالقوانين والمراسيم السلطانية ذات الصلة المعمول بها في سلطنة عمان.





الفصـــــــل الثالث

5. متطلبـات وواجبـات الموظـف

6. مسؤوليات الموظف

7. تحديد هوية المستخدم والمصادقة

5 متطلبات وواجبات الموظف:

5.1 : يجب على المؤسسة الصحية تعيين مسؤول حماية البيانات الصحية من بين المتخصصين في مجال إدارة المعلومات الصحية، وتحديد اختصاصاته ومسؤولياته وفقا لأحكام هذه السياسة.

5.2: يجب على الموظف إتمام برامج التوعية والتدريب المحددة من قبل المؤسسة الصحية، وتشمل الآتي:

1 - برامج التدريب على الخصوصية والأمن.

2 - برامج التدريب على الحماية من البرامج الضارة.

3 - التدريب على إدارة كلمة المرور.

4 - التدريب على قراءة تنبيهات الخصوصية والأمن الموزعة بشكل دوري.

5.3: يجب على المؤسسة الصحية إعداد بطاقات تعريفية لكل من: الموظفين، وعمال الصيانة والنظافة، والمتدربين، والزائرين، باستخدام أحدث التقنيات، ويراعى اختلاف ألوانها وأشكالها بحسب الفئة، أو طبيعة عمل الموظف، ولا تعطى البطاقة التعريفة للزائر إلا إذا كانت الزيارة خارج أوقات العمل الرسمية

5.4: يجب الالتزام في استعمال البطاقات التعريفية بالآتي:

أولا: بالنسبة للمؤسسة الصحية:

1 - إجراء تفتيش دوري من قبل المسؤول المباشر فيها للتأكد من أن جميع الموظفين يرتدون البطاقات التعريفية الصحيحة وبشكل دائم.

2 - تعطيل الرمز الشريطي (الشفرة) الخاص بالبطاقة التعريفية فورا إخطار التقسيم الإداري المختص بفقدانها.

ثانيا: بالنسبة للموظف:

1 - ارتداء البطاقة التعريفية بشكل بارز حتى يتمكن الغير من رؤيتها بسهولة.

2 - إخطار التقسيم الإداري المختص في المؤسسة الصحية فورا في حال فقدان البطاقة التعريفية.

3 - إعادة البطاقة التعريفية للتقسيم الإداري المختص في المؤسسة الصحية عند انتهاء فترة العمل.

4 - عدم إعطاء البطاقة التعريفية لشخص آخر.

5 - عدم إساءة استخدام البطاقة التعريفية.

5.5 : يجب الالتزام بالمحافظة على أمن الحواسيب الآلية المحمولة واللوحية في المؤسسة الصحية، على النحو الآتي:

أولا: بالنسبة للمؤسسة الصحية:

1 - توفير أقفال سلكية لها قابلة للإغلاق، وإرشاد الموظف إلى طريقة استخدامها.

2 - توفير آلية تتبع فعالة لها في حال إخراجها من مبنى المؤسسة الصحية.

3 - توثيق عهدة جميع الأجهزة الإلكترونية لكل قسم.

ثانيا بالنسبة للموظف:

1 - حفظ الأجهزة في مكان آمن.

2 - إبلاغ التقسيم الإداري المختص بتقنية المعلومات في حال تعرضها للتلف لأي سبب.

3 - إغلاقها عند مغادرة مكان العمل.

4 - ضبطها بالقفل التلقائي بعد فترة قصيرة من عدم الاستخدام.

5 - إعادتها إلى عهدة التقسيم الإداري المعني عند انتهاء فترة عمله.

5.6: يجب الالتزام بضوابط الاستخدام الآمن للحواسب الآلية في المؤسسة الصحية على النحو الآتي:

أولا: بالنسبة للمؤسسة الصحية:

1 - تعليق اسم المستخدم وكلمة المرور الخاصة بالموظف للدخول للجهاز بشكل كامل في حال قيامه بإجازة.

2 - إيقاف اسم المستخدم وكلمة المرور الخاصة بالموظف للدخول للجهاز في حال نقله من المؤسسة الصحية أو إنهاء خدمته أو فصله منها.

ثانيا بالنسبة للموظف:

1 - عدم توصيل أو ربط أجهزة الحاسب الآلي والأجهزة اللوحية غير المملوكة للمؤسسة الصحية بشبكات المؤسسة الصحية إلا إذا توفرت وسائل حماية للأنظمة والبيانات المتوافقة مع معايير أمن المعلومات.

2 - عدم تثبيت برامج غير الموافق عليها من المؤسسة الصحية.

3 - عدم إجراء تعديلات أو تغييرات بجهاز الحاسب الآلي دون الرجوع إلى التقسيم الإداري المختص بتقنية المعلومات.

4 - تسجيل الخروج من جميع الأنظمة والتطبيقات وإغلاق الجهاز كليا فورالانتهاء من العمل.

5 - تغيير كلمات المرور للأنظمة المستخدمة بشكل دوري واستخدام كلمات المرور الموصي بها.

6 - عدم استخدام أي أجهزة أو وسائط خارجية مع أجهزة المؤسسة (فلاشات، محرك الاقراص، هواتف وغيرها).

7 - الإبلاغ عن أي اشتباه في عمل النظام والأجهزة للقسم المعني.

8 - المحافظة على الأجهزة التقنية التي يستخدمها.

9 - عدم استخدام الأجهزة أو البرامج أو الشبكة المعلوماتية لأي غرض آخر لا يتعلق بالعمل

10 - عدم إفشاء المعلومات، وكلمات السر الخاصة بدخول الأجهزة.

11 - التقيد بمتطلبات الملكية الفكرية لهذه الأجهزة والبرامج والملفات وشروط استخدامها.

5.7: يحظر على الموظف الآتي:

1 - التسبب في تعطيل نظام المعلومات بسبب عدم اتباع إجراءات الاستخدام الصحيحة.

2 - تجاوز أمن تقنية المعلومات أو تجاوز ميزة أمنية، ويتضمن ذلك تشغيل برامج اختراق كلمات المرور، ومحاولة التحايل على أذونات الملفات أو الموارد الأخرى أو محاولة تنزيل أي برنامج غير مسموح بها دون الرجوع إلى التقسيم الإداري المختص بتقنية المعلومات.

3 - إدخال أو محاولة إدخال فيروسات أو تعليمات برمجية ضارة في نظام المعلومات.

4 - محاولة الاطلاع على معلومات، أو استخدام معلومات لم يتم منحه حق الوصول إليها.

5 - إساءة استخدام الصلاحيات المصرح له بها في أي غرض.

6 - استخدام البرامج الشخصية غير المعتمدة من قبل المؤسسة الصحية.

7 - العبث المادي بالأجهزة وعدم استخدامها الاستخدام الأمثل ومحاولة تصليحها دون خبرة أو معرفة مسبقة.

8 - انتهاك أو محاولة انتهاك شروط الاستخدام أو اتفاقية الترخيص لأي منتج برمجي تستخدمه المؤسسة الصحية.

9 - المشاركة في أي نشاط مخالف للوائح المؤسسة الصحية والقوانين والمراسيم السلطانية واللوائح النافذة، كإرسال أو تبادل المعلومات السرية لغير الأغراض المصرح بها.

6 مسؤوليات الموظف:

6.1: تكون جميع أنظمة الاتصالات الإلكترونية والرسائل التي يتم إنشاؤها أو التعامل معها من خلال أجهزة الحاسب الآلي المملوكة للمؤسسة الصحية، ملكا للمؤسسة الصحية. وتسري هذه السياسة على جميع الاتصالات الإلكترونية التي تتم من خلالها، ويشمل ذلك الهاتف، والبريد الإلكتروني، والبريد الصوتي، والرسائل الفورية، والإنترنت والفاكس، والخوادم.

6.2: يجب في كافة الاتصالات الإلكترونية، الالتزام بالضوابط الآتية:

أولا: بالنسبة للمؤسسة الصحية:

يحق لها مراجعة ملفات الموظف واتصالاته إلكترونية بالقدر اللازم لضمان استخدام جميع الوسائط والخدمات الإلكترونية بما يتوافق مع لوائح المؤسسة الصحية والقوانين والمراسيم السلطانية واللوائح المعمول بها في سلطنة عمان.

ثانيا: بالنسبة للموظف:

1 - عدم استخدام البريد الإلكتروني للمؤسسة الصحية في تسجيل عضوية في أي موقع لا يخدم العمل، لتجنب أي خطر أمني على أنظمة المؤسسة.

2 - عدم توزيع أو تبادل البيانات والمعلومات بدون تصريح مسبق من التقسيم الإداري المختص في المؤسسة الصحية.

3 - جواز الاستخدام الشخصي العرضي للشبكات والبريد الإلكتروني وبرامج وخدمات الإنترنت المخصصة لأغراض العمل، وذلك بما لا يؤثر على إنتاجيته ، وبما لا ينطوي على الآتي:

أ- انتهاك حقوق الطبع والنشر، كاستخدام البرامج والكتب ومقاطع الفيديو المقرصنة، والنَّسَخْ غير القانوني، وتوزيع المعلومات وغيرها مما يندرج المدرجة تحت حقوق النشر.

ب- استخدام موارد أو معلومات المؤسسة الصحية لدعم أغراض غير قانونية.

ت- استخدام موارد أو معلومات المؤسسة الصحية لتحقيق ربح شخصي أو تجاري.

ث- استخدام موارد أو معلومات المؤسسة الصحية لأنشطة سياسية.

ج- استخدام موارد أو معلومات المؤسسة الصحية بطرق مزعجة أو مسيئة للآخرين أو ضارة بالروح المعنوية كالإيحاءات الجنسية أو الإهانات العرقية أو التعليقات العنصرية أو أي شيء يمكن تفسيره على أنه مضايقة أو عدم احترام للآخرين.

4 - لا يتمتع بأي خصوصية شخصية في حال استخدامه شبكة الإنترنت التابعة للمؤسسة الصحية.

6.3: يجب على الموظف عند استخدام الإنترنت في المؤسسة الصحية الالتزام بالضوابط الآتية:

1 - أن يكون الاستخدام حسب احتياجات العمل، ويحظر استخدامه لأغراض شخصية خارج نطاق العمل إلا بمراعاة الضوابط المنصوص عليها في البند ٦.٣من هذه السياسة.

2 - حسن استخدام نقاط الاتصال بالإنترنت.

3 - احترام حقوق النشر والملكية الفكرية المحلية والدولية، وأخذ الموافقة من الجهة الناشرة إذا كان ذلك مطلوباً في حال الرغبة بالتصفح أو النسخ.

4 - أخذ الاحتياطات اللازمة عند تحميل أي ملفات من الإنترنت والتأكد من خلوها من الفيروسات قدر الإمكان.

5 - عدم نشر كل ما من شأنه الدعوة أو الحث على الجريمة أو العنصرية أو التمييز، أو يتعارض مع الشريعة الإسلامية أو النظام العام أو الآداب العامة.

6 - الحصول على موافقة التقسيم الإداري المختص في المؤسسة الصحية قبل تثبيت أو تنزيل أي برامج أو تطبيقات على أجهزة الحاسب الآلي التابعة لها.

7 - الحصول على موافقة التقسيم الإداري المختص في المؤسسة الصحية قبل إتاحة معلومات المؤسسة على أي جهاز حاسب يمكن أن يتصل بالإنترنت (مثل خادم الويب)، ويشمل ذلك الإخطارات والمذكرات والوثائق والبرامج المملوكة للمؤسسة.

8 - عدم تثبيت أو تنزيل أو مشاهدة الألعاب والأفلام والأغاني وكل ما ليس له علاقة بالعمل بأجهزة الحاسب الآلي الخاصة بالمؤسسة الصحية.

6.4: يجب على الموظف عند تبادل المعلومات الصحية شفويا التقيد بالضوابط الآتية:

1 - عدم مناقشة المعلومات الصحية مع زملاء العمل، أو في وجودهم، أو مع أي موظف من داخل المؤسسة، أو أي شخص من خارجها، ما لم تكن المناقشة جزءا من أداء واجباته الوظيفة، وأن يكون الشخص المتلقي للمعلومات مصرح له بذلك في إطار عمله.

2 - توفير بيئة ذات خصوصية عالية عند مناقشة المعلومات الصحية المحمية مع المريض أو من ينوب عنه.

3 - أخذ موافقة المريض أو من ينوب عنه عند مناقشة المعلومات الصحية في غرف الترقيد العامة.

4 - تجنب مناقشة المعلومات الصحية في مناطق الوصول العام، ويشمل ذلك المصاعد والكافتيريا والردهات والممرات، وغيرها.

5 - عدم الرد على أي استفسارات لوسائل الإعلام إلا من خلال التقسيم الإداري المختص في المؤسسة الصحية.

6.5: يجب على الموظف في حالة حدوث خلل في عمل النظام أو اشتباه في إصابته بفيروس، اتباع الخطوات الآتية:

1- التوقف عن استخدام الحاسب الآلي.

2- عدم القيام بتنفيذ أي أوامر، بما في ذلك أوامر حفظ البيانات.

3- فصل شبكة الإنترنت إذا كان ذلك ممكنا.

4- عدم إغلاق أيا من نوافذ أو برامج الحاسب الآلي.

5- عدم إيقاف تشغيل الحاسب الآلي.

6- تدوين أي سلوك غير معتاد للنظام (كرسائل الشاشة أو استجابات غير عادية للأوامر) والوقت الذي لوحظت فيه لأول مرة.

7- إخطار الموظفين المحيطين بأعطال النظام والتنبيه عليهم بعدم محاولة استخدام الجهاز.

8- إبلاغ التقسيم الإداري المختص في المؤسسة الصحية بالتعامل مع العطل، ويجب على هذا التقسيم التعامل مع العطل وإبلاغ المستخدم بالأسباب والإجراءات اللازمة لتفادي العطل مرة أخرى.

6.6: يجب على الموظف إبلاغ التقسيم الإداري المختص بإدارة المعلومات الصحية في المؤسسة بجميع الحوادث الأمنية والانتهاكات فور وقوعها، ويجب على هذا التقسيم بالتنسيق مع التقسيمات المعنية اتخاذ الضوابط التالية:

1- توثيق جميع الحوادث والانتهاكات المبلغ عنها.

2- تحليل كل حادثة أو انتهاك وتحديد مسبباتهما.

3- التواصل مع الجهات المختصة بأمن المعلومات على المستوى الوطني للمساعدة في معالجة الحادث الأمني.

4- توفير التدريب اللازم على أي تغييرات إجرائية تكون مطلوبة في ضوء نتيجة التحقيق في الحادث أو الانتهاك، وإبلاغ الموظفين بأسباب المشكلة، وكيفية تجنبها مستقبلا.

5- تحديث القواعد والإجراءات بشكل دوري، وإضافة الحوادث التي قد تطرأ وكيفية التعامل معها.

6.7: يجب على الموظف في حالة نقل المعلومات السرية، الالتزام بالضوابط الآتية:

1- المعرفة المسبقة بطبيعة وحساسية المعلومات الموجودة في المؤسسة الصحية.

2 - الحفاظ على خصوصية وأمن المعلومات وفقاً للشروط التي تفرضها هذه السياسة.

3 - عدم الإفصاح عن المعلومات لغير الأشخاص المصرح لهم، وعدم الدخول فيما يجاوز نطاق إطار صلاحياته.

6.8: يجب على الموظف في حال تنزيل البرامج والملفات على أجهزة الحاسب الآلي الخاصة بالمؤسسة الصحية، الالتزام بالضوابط الآتية:

1- عدم استخدام البرامج الشخصية على أجهزة الحاسب الآلي أو الشبكات الخاصة بالمؤسسة، إلا إذا كانت هناك حاجة للبرامج والملفات المراد تنزيلها، وبعد الحصول على موافقة التقسيم الإداري المختص في المؤسسة.

2 - عدم استخدام أي برامج خاصة بالمؤسسة في المنزل أو على أجهزة الحاسب الآلي غير التابعة للمؤسسة إلا بتصريح من التقسيم الإداري المختص في المؤسسة.

3 - عدم وضع بيانات الملكية الخاصة بالمؤسسة على أجهزة الحاسب الآلي غير التابعة للمؤسسة، بما في ذلك معلومات المريض، ومعلومات أنظمة تكنولوجيا المعلومات، والمعلومات المالية، وبيانات الموارد البشرية، إلا بتصريح من التقسيم الإداري المختص في المؤسسة.

4 - عدم استخدام أو تداول برامج تخضع للملكية الفكرية دون تصريح مسبق من أصحابها.

5 - التخلص من البرامج ذات الطابع التجريبي فور انتهاء الفترة التجريبية.

6 - تحديث البرامج بشكل دوري للإصدار الأحدث لتفادي أي أخطار قد تتعلق بالقرصنة أو الأخطاء الفنية للأنظمة وتفادي ظهور مشاكل في التوافق مع باقي الأنظمة.

7 - استخدام برامج ذات طابع أمني (اسم مستخدم ورقم سري) للمحافظة على سرية الملفات وضمان عدم تسربها.

8 - ملاءمة الاحتفاظ بأكثر من نسخة لنفس الملف وفي نفس المجلد.

9 - عدم ملاءمة استخدام مساحات تخزينية خاصة لحفظ الملفات مع وجود ميزة النسخ الاحتياطي لضمان عدم ضياعها وتلفها.

10 - الاستخدام الدوري لمضاد الفيروسات لضمان سلامة الملفات.

11 - تحديث البرامج المضادة للفيروسات وجميع البرمجيات الأخرى المتاحة عبر الشبكة.

12 - العلم بعدم تتمتع أجهزة الحاسب الآلي الشخصية غير التابعة للمؤسسة الصحية والمعلومات والبيانات المحفوظة فيها والبرامج والأنظمة المثبتة فيها بحماية المؤسسة، لعدم قدرة المؤسسة على التحكم فيها أو التأكد من أساليب الحماية الموجودة فيها.

6.9: يجب على الموظف عند استخدام برامج الملفات المضغوطة بغرض تسهيل حفظ الملفات ونقلها كحزمة واحدة، مراعاة الضوابط الآتية:

1 - تبادل المفاتيح الخاصة بتشفير وفك تشفير كل عملية إرسال عند تبادل الملفات عبر البريد الإلكتروني.

2 - طلب برامج الملفات المضغوطة من التقسيم المختص في المؤسسة.

6.10: يجب على الموظف في حال الحاجة إلى إخفاء هوية المريض ،الالتزام بحذف جميع المعرفات الخاصة بالمريض قبل تبادل أو استخدام معلوماته الشخصية لأغراض البحث أو الإحصاء، وتشمل تلك المعرفات الاسم، ورقم السجل الطبي، ورقم الهاتف، ورقم الفاكس، وعنوان البريد الإلكتروني، والرقم المدني، والصورة الفوتوغرافية، وعنوان المنزل، وجميع عناصر التواريخ المرتبطة مباشرة بالفرد (تواريخ الميلاد، والزواج، والوفاة، وغيرها).

7 تحديد هوية المستخدم والمصادقة:

7.1: يجب على المؤسسة الصحية أخذ توقيع الموظف والمستخدمين المؤقتين والمتدربين بالموافقة على وثيقة الحفاظ على سرية المعلومات الصحية، والتي تشمل الآتي:

1 - أن أي استخدام أو إفشاء غير مصرح به للمعلومات قد يؤدي إلى اتخاذ إجراءات تأديبية قبله وفقا للوائح والقوانين والمراسيم السلطانية المعمول بها.

2 - أن يتم التوقيع بالموافقة على الوثيقة قبل الدخول إلى النظام.

3 - مراجعة وتحديث وثيقة الحفاظ على السرية كلما اقتضت الحاجة إلى ذلك.

4 - ملاءمة توفير شاشة على النظام تظهر بشكل دوري لتذكير الموظفين باللوائح والقواعد واجبة الاتباع.

7.2: يجب على المؤسسة الصحية التحكم في الوصول إلى المعلومات الصحية، وذلك اتباع الضوابط الآتية:

1 - استخدام أنظمة التحكم في الدخول إلى النظام، وتنقسم إلى نوعين كالآتي:

أ- أنظمة داخلية: وتشمل كلمات المرور، والتشفير، والتحكم في الوصول لكل مستخدم

ب- أنظمة خارجية: وتشمل أجهزة حماية المنفذ والجدران النارية، والحماية من الفيروسات وأنظمة منع تسرب البيانات.

2 - توفير إجراءات أمنية إضافية للحد من وصول الموظف إلى المعلومات عالية الحساسية.

3 - تحديد صلاحيات الموظف في ضوء مسؤولياته ومهامه الوظيفية، وبناء على المعايير المحددة من قبل المؤسسة.

4 - تضمين صفحة دخول أنظمة المؤسسة إشعار تنبيه يفيد حظر الاستخدام غير المصرح به أو محاولة انتهاك لوائح خصوصية وأمن المعلومات بأي شكل من الأشكال، وأن المخالفين سيخضعون للمساءلة القانونية.

7.3: يجب على المؤسسة الصحية توفير نظام تحكم معرفات المستخدم، بغرض التعرف على كل مستخدم ونطاق صلاحياته للدخول للأنظمة واستخدام المعلومات والبيانات، مع وجوب مراعاة الآتي:

1 - تحديد التقسيم الإداري المختص في المؤسسة الصحية بإدارة معرفات المستخدمين وكلمات المرور.

2 - تعيين معرف فريد لكل مستخدم.

3 - عدم تعيين معرف بأسماء أقسام أو جهات عمل.

4 - تحميل كل مستخدم مسؤولية استخدام أو إساءة استخدام معرف تسجيل الدخول الخاص به.

5 - تدقيق أو تغيير كافة معرفات تسجيل دخول المستخدمين مرتين سنويًا على الأقل.

6 - إيقاف حساب المستخدم بشكل مؤقت بعد ثالث محاولة غير ناجحة لتسجيل الدخول كحد أقصى، يجب بعدها إعادة تعيين كلمة المرور حسب الآلية المتبعة من قبل المؤسسة.

7 - إيقاف كافة معرفات تسجيل الدخول غير النشطة إذا تجاوزت (180) مائة وثمانون يومًا من عدم النشاط.

8 - عدم السماح باستخدام معرفات تسجيل دخول المستخدم في أكثر من جهاز بنفس الوقت.

7.4: يجب على المستخدم، تحديد كلمة مرور للدخول إلى النظام الإلكتروني يراعى فيها المعايير والضوابط الآتية:

1 - تغيير كلمة المرور التلقائية المعطاة من قبل النظام مباشرة عند تسجيل الدخول للنظام لأول مرة.

2 - ألا تقل كلمة المرور عن (8) ثمانية رموز.

3 - أن تحتوي كلمة المرور على مجموعة من الرموز الأبجدية الكبيرة والصغيرة والرموز الرقمية والرموز المميزة.

4 - تغيير كلمة المرور كل (180) مائة وثمانين يومًا.

5 - تغيير كلمات المرور المخترقة على الفور.

6 - عدم إعادة استخدام كلمة المرور السابقة عند إعادة تعيينها خلال (1) سنة واحدة من آخر استخدام.

7 - عدم استخدام الأسماء أو الأحرف الأولى منها أو أعياد الميلاد أو أرقام الهواتف شائعة الاستخدام ككلمات مرور.

8 - عدم مشاركة كلمة المرور أو تدوينها على الورق أو تخزينها في ملف أو قاعدة بيانات.

9 - إخفاء كلمات المرور ومنع عرضها على الشاشات بتنسيق مشفر، ولا يتم طباعتها أو تضمينها في التقارير والسجلات.

10 - وضع كلمة مرور فريدة لكل برنامج، مع عدم استخدام نفس كلمة المرور لجميع البرامج والتطبيقات بالمؤسسة.

7.5: يجب تحديد صلاحيات المستخدمين للدخول إلى أنظمة المؤسسة الصحية بمراعاة الآتي:

1 - أن يتم التحديد من قبل التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات.

2 - أن يتم التحديد في ضوء اختصاصات ومسؤوليات الوظيفية، والمعايير المحددة من قبل المؤسسة الصحية.

3 - في حال تغيير صلاحيات المستخدم، يجب على الرئيس المباشر للموظف إخطار التقسيم الإداري المختص بإدارة المعلومات الصحية بالصلاحيات الجديدة للموظف، وأن تكون بالقدر الذي يمكن الموظف من الوصول إلى الحد الأدنى من البيانات الضرورية لأداء واجباته أداءً فعّالاً.

4 - أن يحتوي كل نظام من أنظمة المؤسسة على صفحة تحكم لإدارة صلاحيات المستخدمين تتيح التأكد من حيازة كل موظف الحد الأدنى من الصلاحيات.

5 - مراجعة صلاحيات المستخدمين سنوياً من قبل التقسيم الإداري المختص بإدارة المعلومات الصحية مع الرئيس المباشر للتأكد من أن جميع المستخدمين لديهم الحد الأدنى من الصلاحيات لإداء مهامهم بفعالية.

6 - يحق للتقسيم الإداري المختص بإدارة المعلومات الصحية - من تلقاء نفسه - تغيير أو سحب صلاحيات المستخدم بما يتوافق مع الواجبات الوظيفية للموظف.

7.6: يجب على المؤسسة الصحية تجميد حساب المستخدم (غلقه مؤقتا) في الحالات ووفقا للضوابط الآتية:

1 -أن يتم التجميد من قبل التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية بناء على طلب المستخدم، أو تجميد الحساب تلقائيا من خلال ربط الأنظمة الصحية مع نظام الموارد البشرية.

2 - أن يكون التجميد في حال الترخيص للمستخدم بإجازة.

3 - بدلا من تجميد حساب المستخدم، يجوز للتقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية بناء على طلب الرئيس المباشر ، منح صلاحيات الدخول للحساب لمن ينوب عن المستخدم في واجبات وظيفته لحين عودته من الإجازة.

4 - التأكد من سحب الصلاحيات الممنوحة للموظف البديل فور عودة صاحب الصلاحيات من الإجازة.

7.7: يجب على المؤسسة الصحية غلق حساب المستخدم نهائيا في الحالات، ووفقا للضوابط الآتية:

1 - أن يتم الغلق من قبل التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية بناء على طلب الرئيس المباشر للمستخدم، أو يتم الغلق تلقائيا من خلال ربط الأنظمة الصحية مع نظام الموارد البشرية في المؤسسة.

2 - أن يقتصر الغلق النهائي على حالة انتهاء خدمة المستخدم أو علاقته بالمؤسسة الصحية لأي سبب.

3 - أن يقدم التقسيم الإداري المختص بإدارة المعلومات الصحية لرؤساء التقسيمات الإدارية المختلفة – كل فيما يخصه - قائمة بحسابات المستخدمين النشطة (2) مرتين سنوياً للمراجعة، لغرض تنفيذ البند الأول من البند ٧.٧.

4 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات، لتعطيل صندوق البريد الإلكتروني الخاص بالمستخدم المنتهية خدماته أو علاقته بالمؤسسة الصحية، وإخطار كافة المستخدمين الآخرين بعنوان صندوق البريد الإلكتروني للمستخدم الجديد الذي سيحل محله.

الفصـــــــل الرابع

8. معالجة البيانات الصحية

8.1: معالجة البيانات الصحية

8.2: الزام المؤسسة الصحة في معالجة البيانات الصحية

8.3: تصنيف البيانات الصحية

8.4: إنشاء السجل الصحي وتحديثه

8.5: توثيق البيانات الصحية

8.6: الرعاية الصحية عن بعد

8.7: التقاط الصور الفوتوغرافية والتسجيل الصوتي أو المرئي

8.8: تحميل بيانات التصوير الضوئي والتسجيل المرئي وتنزيلها

8.9: المسح الضوئي للبيانات الورقية

8.10: نسخ البيانات الصحية ولصقها

8.11: تعديل البيانات الصحية وحذفها

8.12: دمج السجلات الصحية المتكررة داخل المؤسسة

8.13: حجب البيانات الصحية

8.14: طباعة البيانات من سجل المريض الصحي

8.15: مشاركة البيانات الصحية

8.16: الافصاح عن البيانات الصحية

8.17: إتاحة البيانات المفتوحة

8.18: تجميد السجل الصحي بعد الوفاة

8.19: الاحتفاظ بالسجلات وأرشفتها وإتلافها

8 معالجة البيانات الصحية

8.1: تشمل معالجة البيانات الصحية، عمليات جمع وتسجيل وتحليل وتنظيم وتخزين وتعديل وتحوير واسترجاع ومراجعة وتنسيق وربط وحجب ومحو وإلغاء والإفصاح عن البيانات، عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى وذلك على النحو المبين في البنود التالية.

8.2: تلتزم المؤسسة الصحة في معالجة البيانات الصحية، بالتعاون مع الجهات المختصة، وتقديم ما تطلبه من بيانات ومستندات تراها لازمة لممارسة اختصاصها وفقا لأحكام القوانين والمراسيم السلطانية النافذة.

8.3: تصنيف البيانات الصحية، تلتزم المؤسسة الصحية بتصنيف جميع البيانات والمعلومات الصحية التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها سواء كانت في شكل إلكتروني، أو غير إلكتروني، أيا كان مكان وجود ها أو نوع الجهاز المخزنة فيه، وذلك وفقا للمستويات الآتية:

1 - المعلومات الصحية عالية السرية.

2 - المعلومات الصحية السرية.

3 - المعلومات الصحية العامة (المفتوحة).

8.3.1: المعلومات الصحية عالية السرية، تشمل البيانات الشخصية المتعلقة بالصحة الجسدية، والعقلية والنفسية للمريض، وتتطلب استخدام معايير مناسبة لضمان خصوصية وأمن المعلومات، وذلك على النحو الآتي:

1 - أن يكون الوصول إليها وفقا للضوابط المنصوص عليها في البند ٧.٢ من هذه السياسة.

2 - يتم تصنيفها بحسب درجة حساسيتها إلى الآتي:

أ- عالية الحساسية: كالأمراض النفسية والأمراض المعدية وحالات الإدمان والاعتداءات والجرائم والانتحار والصور الفوتوغرافية والتسجيل الصوتي أو المرئي والبيانات الجينية.

ب- حساسة: جميع محتويات السجل الصحي للمريض.

3 - لا يسمح بالوصول إليها إلا للفريق الطبي الموثق للمعلومة.

4 - أن يكون التعامل معها بخصوصية عالية.

5 - أن يقتصر الترخيص بالوصول إليها على الحد الأدنى الضروري لإداء مهام العمل.

8.3.2: المعلومات الصحية السرية، هي المعلومات التي تشمل بصفة خاصة الآتي:

1 - البيانات الشخصية للمرضى: كالرقم المدني، ورقم المقيم، ورقم السجل الصحي، ورقم الهاتف وبيانات الضمان الاجتماعي، ورقم بطاقات الائتمان.

2 - بيانات المصادقة: كمفاتيح التشفير الخاصة، واسم المستخدم، وكلمة المرور.

3 - السجلات المالية: كأرقام الحسابات المالية.

4 - البريد الإلكتروني، ومعظم الرسائل التي يمكن حذفها أو نشرها دون أن تتسبب في أضرار.

5 - أي معلومات لا تصنف على أنها معلومات عالية السرية.

8.3.3: البيانات الصحية المفتوحة (العامة)، هي البيانات التي يمكن الكشف عنها للعامة كالخدمات التي تقدمها المؤسسة الصحية، والكوادر التخصصية المتوفرة لديها، والإحصائيات العامة.

8.4: إنشاء السجل الصحي وتحديثه، يجب على المؤسسة الصحية في إنشاء وتحديث السجل الصحي للمريض، الالتزام بالضوابط الآتية:

1 - توفير الأدوات التقنية المتقدمة لتفادي إنشاء أكثر من سجل لمريض واحد.

2 - استخدام البطاقة الشخصية، أو بطاقة المقيم عند تسجيل المريض.

3 - التحقق من تطابق بيانات البطاقة الشخصية، أو بطاقة المقيم مع شخص المريض.

4 - استيفاء الحد الأدنى من البيانات الديموغرافية للمريض، وبصفة خاصة الآتي:

أ- الرقم المدني، أو رقم المقيم.

ب- الاسم الأول والثاني والثالث والقبيلة للعمانيين.

ج- الاسم الأول والثاني للمقيم.

د- تاريخ الميلاد.

هـ - الجنسية.

و- الجنس.

ز- الحالة الاجتماعية.

ح- مكان الإقامة.

ط- رقم الهاتف.

ي - جهة العمل.

ك- المهنة.

ل- الديانة.

م- اسم أحد الأقارب.

ن- رقم هاتف أحد الأقارب.

5 - تحديث البيانات الديموغرافية للمريض عند كل زيارة والتأكد من صحتها.

6 - تحصيل الرسوم اللازمة (إن وجدت) عند تسجيل الزيارة.

8.5: توثيق البيانات الصحية، يجب على المؤسسة الصحية توثيق البيانات الصحية للمريض، ويكون التوثيق إما نشطا أو غير نشط، وذلك على النحو المبين في البندين التاليين:

8.5.1: التوثيق النشط، يتم التوثيق النشط للبيانات في أثناء فتح الزيارة، سواء في حال حضور المريض شخصيا أو في حال تقديم الرعاية الصحية له عن بعد، وذلك بالالتزام بالضوابط الآتية:

1 - يكون توثيق البيانات من قبل أعضاء الفريق الطبي المشرف على العلاج دون غيره.

2 - أن يتم التوثيق من خلال اسم المستخدم الخاص بالموثق دون غيره.

3 - التأكد من أن التوثيق يتم في السجل الصحيح.

4 - التأكد من أن سجل المريض يحتوي على الحد الأدنى من البيانات، ويشمل ذلك المشاكل الصحية، والتقييم، والفحوصات المختبرية، والوصفات الطبية، والإحالات، وأي إرشادات تم تقديمها.

5 - عدم ذكر نوع المرض في شهادة الأجازة المرضية، إلا بموافقة المريض أومن ينوب عنه، أو تنفيذا لنص في قانون أو مرسوم سلطاني.

6 - قيام رئيس الفريق الطبي المعالج بالمصادقة على توثيق أعضاء فريقه كلما تطلب الأمر ذلك.

7 - إتمام التوثيق مباشرة وبالتزامن مع تقييم وعلاج وتطور حالة المريض.

8 - أن تكون البيانات التي تم توثيقها صحيحة وواضحة، ومكتملة، وشاملة، ومترابطة.

9 - يمكن لأحد أعضاء الفريق الطبي المعالج التوثيق من خارج المؤسسة الصحية في حالات الاستشارة عن بعد، شريطة توفر نظام إلكتروني آمن، وبمراعاة متطلبات وضوابط العمل عن بعد المنصوص عليها في البند ١٠.٢ من هذه السياسة.

8.5.2: التوثيق غير النشط، يتم التوثيق غير النشط للبيانات في غير أوقات الزيارة المفتوحة للمريض من خلال إضافة ملحق إلى سجل المريض، وذلك بالالتزام بالضوابط الآتية:

1 - عدم استخدام التوثيق غير النشط إلا في حالات محدودة، كتوثيق مستجدات حالة المريض وعمليات التواصل من خلال الهاتف.

2 - ذكر أسباب التوثيق غير النشط.

3 - تتبع أسباب التوثيق غير النشط من خلال التقسيم الإداري المختص بإدارة المعلومات الصحية.

8.6: الرعاية الصحية عن بعد، تعد من أهم أساليب التواصل الحديث الذي يسهل التواصل بين الكادر الطبي المعالج والمريض لمعاينته وتشخيصه وتقديم الاستشارة الطبية له من مكان إقامته، كما أنها وسيلة سهلة وفعالة للتواصل بين الكوادر الطبية لتقديم الاستشارات و عقد المؤتمرات العلمية والأنشطة التعليمية الطبية الأخرى، وذلك من خلال منظومة إلكترونية صوتيه ومرئية ومعلوماتية، وتسمى «الطلب الاتصالي».

8.6.1: تصنف الرعاية الصحية عن بعد ، على النحوالآتي:

1 - الاستشارة عن بعد.

2 - التشخيص عن بعد.

3 - استشارة خبير عن بعد.

4 - الإشراف الطبي عن بعد.

5 - المساعد عن بعد.

6 - مراقبة المريض عن بعد.

7 - الجراحة عن بعد.

8.6.2: يلزم لممارسة الرعاية الصحية عن بعد، الالتزام بالضوابط التقنية والأمنية والضوابط العامة المبينة في البندين التاليين:

8.6.2.1: تتمثل الضوابط التقنية والأمنية للرعاية الصحية عن بعد في الآتي:

1 - أن يشمل عقد شراء التطبيقات الخاصة بالرعاية الصحية عن بعد الدعم الفني أو اتفاقية مستوى الخدمة.

2 - أن تكون تطبيقات الرعاية الصحية عن بعد مستضافة في شركات الاتصال ومراكز البيانات المعتمدة محليا.

3 - أن يوفر مزود الخدمة تطبيقات تعمل في أجهزة الحاسب الآلي والأجهزة اللوحية والمحمولة.

4 - أن تتوفر في خاصية الرعاية الصحية عن بعد خاصية التسجيل المسبق من خلال اسم المستخدم ورمز المرور للدخول إلى التطبيق.

5 - استخدام طرق التشفير التي تضمن خصوصية وأمن البيانات عند تبادلها أثناء الرعاية الصحية عن بعد.

6 - الالتزام بالتحديثات الدورية للتطبيقات المستخدمة في الرعاية الصحية عن بعد.

7 - أن تحتوي الأجهزة المستخدمة لنقل البيانات على برامج آمنة ومحدثة للحماية من الهجمات الإلكترونية.

8 - تعريف بروتوكول في حال حدوث عطل تقني او توقف النشاط.

8.6.2.2: تتمثل الضوابط العامة لممارسة الرعاية الصحية عن بعد في الآتي:

1 - حصول المؤسسة الصحية على ترخيص لممارسة الرعاية الصحية عن بعد من الوزارة.

2 - التزام الكادر الطبي المعالج بالتأكد من هوية المريض بأدلة كافية عن طريق السؤال عن اسم المريض أو عمره أو عنوانه أو رقم الهاتف.

3 - التزام الكادر الطبي المعالج بتعريف المريض بهويتهم لبث الاطمئنان في نفسه.

4 - إدراج جميع تفاصيل الرعاية الصحية عن بعد في ملف المريض الطبي وتشمل الآتي:

أ- هوية الفريق الطبي المعالج.

ب- نوع (تصنيف) الرعاية الصحية عن بعد.

ج- موقع المريض عند تقديم الرعاية الصحية له عن بعد.

د- تاريخ ووقت تقديم الرعاية الصحية للمريض عن بعد.

هـ- المشاكل الصحية، والتقييم، والفحوصات المختبرية، والوصفات الطبية، والإحالات وأي إرشادات تم تقديمها للمريض.

و- جميع الحوادث التقنية التي من شأنها التأثير على نشاط الرعاية الصحية عن بعد.

5 - حفظ تفاصيل توثيق جلسة الرعاية الصحية عن بعد بشكل تسلسلي مع الزيارات السابقة في السجل الطبي للمريض.

6 - تقديم الرعاية الصحية عن بعد في مكان يكفل الخصوصية التامة للمريض.

7 - أخذ موافقة المريض عند الحاجة لتسجيل جلسة العلاج لأغراض البحوث والتعليم.

8 - خضوع أي عملية تصوير فوتوغرافي أو تسجيل صوتي أو مرئي أثناء ممارسة الرعاية الصحية عن بعد للبند 8.7 من هذه السياسة.

9 - أن تكون جميع الوثائق الطبية في متناول المريض عند حاجته إليها.

10 - أن يكون لدى المؤسسة الصحية خطة احتياطية بشأن كيفية التواصل مع المريض في حالة حدوث فشل تقني، وأن يكون المريض على دراية بها.

11 - التزام الكادر الطبي بتحديد موعد للمريض لزيارة المستشفى إذا كان يعتقد لأي سبب من الأسباب أن الرعاية الصحية عن بعد تشكل خطراً على سلامة المريض.

12 - عدم السماح للكادر الطبي في حالات الطوارئ، بتأخير إحالة المريض ومحاولة تشخيص الحالة وتقديم العلاج له عن بعد.

13 - التزام الكادر الطبي بمناقشة حالة المريض مع أطباء آخرين أكثر خبرة وأدق تخصصا كلما قدروا الحاجة إلى ذلك، ثم الاتصال بالمريض في أقرب وقت ممكن

14 - سريان كافة القواعد القانونية المطبقة على الكادر الطبي في سلطنة عمان على الكوادر الطبية التي تمارس الرعاية الصحية عن بعد.

15 - أن يتم تسجيل الكادر الطبي المتواجد خارج سلطنة عمان الراغبين في ممارسة الرعاية الصحية عن بعد للمرضى المتواجدين في سلطنة عمان لدى الوزارة، ويعد هذا الكادر مسؤولا عن كافة أفعاله أمام السلطات القضائية وفقا للنظام القانوني الخاضع له.

16 - سريان اللوائح الخاصة بالتغطية التأمينية الصحية في سلطنة عمان على التغطية التأمينية الصحية لإجراءات الرعاية الصحية عن بعد.

17 - خضوع الكادر الطبي للتدريب قبل ممارسة الرعاية الصحية عن بعد.

18 - يجب ان يحتوي تأمين الأخطاء الطبية للكادر الطبي على ممارسات الرعاية الصحية عن بعد.

19 - أن تكون لدى الكادر الطبي المعالج إمكانية الوصول الى جميع المعلومات الصحية ذات الصلة في حال تواجدها.

20 - أن يتم أخذ موافقة المريض على الرعاية الصحية عن بعد من خلال نموذج الموافقة، ويفضل ان يكون إلكترونيا.

21 - يحق للمريض رفض أو إلغاء أي مشاركة في نشاط الرعاية الصحية عن بعد في أي وقت دون الحاجة الى تقديم مبررات.

22 - أن يتلقى المرضى توعيه وتدريب بخصوص نشاط الرعاية الصحية عن بعد إذا لزم الامر.

23 - التزام المؤسسة الصحية بتعريف بروتوكول في حال حدوث حالة طبية طارئة خلال تقديم الرعاية الصحية عن بعد.

8.7: التقاط الصور الفوتوغرافية والتسجيل الصوتي أو المرئي، يجب على الكادر الطبي عند الحاجة لالتقاط صور فوتوغرافية أو إجراء تسجيل صوتي أو مرئي، مراعاة الضوابط الآتية:

1 - استخدام نموذج الموافقة الكتابية لتوثيق موافقة المريض أو من ينوب عنه، ويستثنى من ذلك:

أ- صور الشرائح المختبرية والأشعة السينية والموجات فوق الصوتية.

ب- الصور بالمنظار.

ج- صور الأعضاء الداخلية للجسم.

د- تسجيلات وظائف الأجهزة الداخلية للمريض.

2 - عدم استخدام الصور أو التسجيلات الصوتية أو المرئية لأغراض خارج نطاق الموافقة الأصلية، وإلا وجب الحصول على موافقة أخرى.

3 - يقتصر إجراء التصوير الفوتوغرافي والتسجيل الصوتي أو المرئي في الحالات الآتية:

أ- أن يكون التصوير أو التسجيل جزءا من التقييم أو التحقيق أو العلاج للمريض، على أن يتم حفظه في السجل الطبي للمريض.

ب- لغرض إعداد دليل محتمل، في حال الإصابات نتيجة حادث أو اعتداء وغيرهما.

ج- للاستخدام في التدريس أو التدريب أو تقييم المهنيين الصحيين والطلاب أو المجموعات الأخرى، كالمؤتمرات.

د- للاستخدام في البحوث السريرية.

هـ - للنشر، في كتاب أو مجلة أو نشرة عن معلومات للمريض أو على ملصق أو في مواد دعائية، ويمكن الوصول إلى أي منها عبر الإنترنت.

4 - إبلاغ المريض أو من ينوب عنه بالآتي:

أ- ما سيتم تصويره أو تسجيله، مرئياً أو صوتياً.

ب- الغرض من التسجيل أو التصوير، ومن سيشاهده.

ج- الظروف التي سيتم فيها استخدام التسجيل أو التصوير، ومدى إمكان سحبة بعد اتاحته في المجال العام.

د- عمل نسخ والمحافظة على السرية التامة للبيانات وموقع الحفظ.

5 - إبلاغ المريض بأن له الحرية المطلقة في إيقاف التسجيل في أي وقت أو سحب موافقته، دون أن يؤثر ذلك على جودة الرعاية التي يتلقاها، وإبلاغه أيضا بحقه في المشاهدة أو الاستماع إليها إذا رغب في ذلك، قبل اتخاذ قرار بشأن الموافقة على استخدامها، فإذا قرر المريض عدم موافقته على استخدام أي تسجيل، فيجب إتلافه في أسرع وقت ممكن.

6 - أن يتم حفظ الصور الفوتوغرافية والتسجيلات الصوتية والمرئية كجزء من سجل المريض الصحي.

7 - توفير إجراءات أمنية إضافية للحد من وصول المستخدمين إلى الصور الفوتوغرافية والتسجيلات الصوتية والمرئية.

8.8: تحميل بيانات التصوير الضوئي والتسجيل المرئي وتنزيلها، يجوز للمؤسسة الصحية تحميل، أو تنزيل بيانات التصوير الضوئي أو المرئي من وإلى السجل الصحي للمريض، وتشمل هذه البيانات التصوير الطبي الضوئي والتسجيل المرئي بكافة أنواعه والإجراءات التشخيصية والعلاجية المختلفة، ويجب على المؤسسة توفير الأدوات اللازمة لذلك.

8.8.1: تحميل بيانات التصوير الضوئي والتسجيل المرئي، يجب أن يكون تحميل بيانات التصوير الضوئي والتسجيل المرئي، وفقا للضوابط الآتية:

1- ينصب التحميل على البيانات التي يتم إنشاؤها من خارج المؤسسة الصحية.

2- أن يكون التقسيم الإداري المختص بإدارة المعلومات الصحية مسؤولا عن تحميل البيانات

3- إرسال البيانات حسب الحاجة إلى التقسيم الإداري المختص بإدارة المعلومات الصحية.

4- أن تكون بيانات التي تم تحميلها مربوطة بالسجل الصحي للمريض.

5- أن تكون البيانات منظمة وسهل الوصول إليها عند الحاجة.

6- إعادة البيانات للمريض أو من ينوب عنه فور الانتهاء من عملية التحميل.

8.8.2: تنزيل بيانات التصوير الضوئي والتسجيل المرئي، يجب أن يكون تنزيل بيانات التصوير الضوئي والتسجيل المرئي، وفقا للضوابط الآتية:

1- أن يكون تنزيل البيانات بطلب من المريض أو من ينوب عنه قانونا.

2- أن يكون التقسيم الإداري المختص بإدارة المعلومات الصحية هو المسؤول عن تنزيل البيانات.

3- تحصيل الرسوم المقررة لخدمة تنزيل البيانات إن وجدت.

4- مراعاة خصوصية وسرية البيانات عند التنزيل.

8.9: المسح الضوئي للبيانات الورقية، يجب على المؤسسة الصحية إجراء مسح ضوئي لجميع البيانات الطبية الورقية، سواء كان مصدرها من داخل المؤسسة أو من خارجها، وذلك وفقا للضوابط الآتية:

1- يتولى التقسيم الإداري المختص بإدارة المعلومات الصحية إجراء المسح الضوئي للبيانات الطبية الورقية.

2 - أن يتم المسح الضوئي للبيانات الطبية الورقية بصورة دورية.

3 - التزام الأقسام الطبية في المؤسسة بإرسال البيانات الورقية الطبية بصورة دورية الى التقسيم الإداري المختص بإدارة المعلومات الصحية.

4 - أن تكون البيانات الورقية الطبية مربوطة بالسجل الصحي الإلكتروني للمريض.

5 - أن تكون البيانات الورقية الطبية منظمة ومفهرسة وسهل الوصول إليها عند الحاجة

6 - أن يكون التخلص من البيانات الطبية الورقية التي تم مسحها بطريقة آمنة تكفل حماية خصوصية وسرية البيانات.

8.10: نسخ البيانات الصحية ولصقها، يجوز للمؤسسة الصحية استخدام أداة نسخ ولصق البيانات في حالات محدودة، ووفقا للضوابط الآتية:

1 - اقتصار نسخ ولصق البيانات في نطاق السجل الصحي للمريض نفسه.

2 - عدم نسخ ولصق البيانات من مصدر خارج السجل الصحي للمريض.

3 - توخي الحذر من قبل موثق البيانات عند إعادة استخدام البيانات من خلال النسخ واللصق، والتحقق من أنها تنطبق بالفعل على الزيارة الحالية بالرجوع إلى المريض.

4 - تجنب تكرار نسخ ولصق البيانات غير الضرورية.

5 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بمراقبة وقياس وتقييم عمليات النسخ واللصق بشكل دوري من خلال توفير أداة تقنية تتيح للمستخدم التعرف على تفاصيل النسخ واللصق بما في ذلك الآتي:

أ- مصدر البيانات المنسوخة

ب- اسم المستخدم الذي قام بتوثيق البيانات المنسوخة.

ج- تاريخ توثيق البيانات المنسوخة.

6 - توفير التدريب والتعليم المناسبين للموظفين فيما يتعلق بالاستخدام المناسب والآمن لخاصية النسخ واللصق.

8.11: تعديل البيانات الصحية وحذفها، يجوز للمريض طلب تعديل بياناته الصحية وبياناته الديموغرافية وفقا للضوابط المنصوص عليها في البنود التالية.

8.11.1: يجوز للمؤسسة الصحية حذف البيانات الصحية للمريض لحاجة العمل، في الحالات الآتية:

1 - وقوع خطأ في تسجيل الزيارة.

2 - وقوع خطأ في توثيق البيانات.

3 - الخلط بين السجلات الصحية.

8.11.2: يجب على المؤسسة الصحية عند حذف البيانات الصحية، الالتزام بالضوابط الآتية:

1 - ألا تكون البيانات المراد حذفها قد تم حفظها في السجل الصحي للمريض.

2 - أن يظهر المحتوى المحذوف بصيغة التعديل بوضع خط على البيانات المحذوفة باستخدام اللون الأحمر لسهولة تمييزها.

3 - أن يكون لدى المؤسسة الصحية إجراءات واضحة تتعلق بحذف البيانات الصحية.

4 - أن يشتمل السجل الصحي للمريض على تفاصيل الحذف، بما فيها الآتي:

أ- البيانات المحذوفة باللون الاحمر.

ب- مبررات الحذف.

ج- اسم المستخدم الذي قام بعملية الحذف.

د- تاريخ وتوقيت الحذف.

5 - توفير تقارير لتعقب عمليات حذف البيانات.

6 - أن تظهر كل البيانات بما فيها البيانات المحذوفة عند الطباعة.

7 - إبلاغ المريض بأي عملية حذف في بياناته الصحية كلما دعت الحاجة لذلك.

8 - أن يتولى التقسيم الإداري المختص بإدارة المعلومات الصحية إدارة ومتابعة عمليات الحذف وإعداد تقارير دورية بذلك.

8.12: دمج السجلات الصحية المتكررة داخل المؤسسة، يجوز للمؤسسة الصحية دمج السجلات الصحية، بمراعاة الضوابط الآتية:

1 - توفير الأدوات التقنية المتقدمة لتفادي خلق أكثر من سجل للمريض الواحد.

2 - وضع إجراءات واضحة ودقيقة لعملية دمج السجلات.

3 - توفير آلية للتمكن من تتبع عملية دمج السجلات.

4 - يتولى التقسيم الإداري المختص بإدارة المعلومات الصحية عملية دمج السجلات.

8.13: حجب البيانات الصحية، يجب على المؤسسة الصحية حجب بيانات السجل الصحي للمريض كلما تطلب الأمر ذلك، وعليها في تلك الحالة توفير أداة فعالة في الحالات وبالضوابط الآتية:

1 - أن يتم حجب البيانات بشكل جزئي أو كامل لدواعي اجتماعية ونفسية وأمنية وسياسية.

2 - أن يتم حجب البيانات التعريفية للمريض في حال استخدام بياناته الصحية لغرض البحوث والدراسات أو أي أغراض أخرى.

3 - أن يتم حجب البيانات من قائمة دليل المستشفى للمرضى المنومين إذ طلب المريض ذلك.

4 - يتولى التقسيم الإداري المختص بإدارة المعلومات الصحية عملية الحجب.

8.14: طباعة البيانات من سجل المريض الصحية، يجب على المؤسسة الصحية في طباعة بيانات السجل الصحي للمريض، الالتزام بالضوابط الآتية:

1 - قصر صلاحيات الطباعة على الطبيب المعالج والموظف المختص بالتقسيم الإداري المختص بإدارة المعلومات الصحية.

2 - قصر الطباعة على البيانات العامة بما فيها ملخص الترخيص، وورقة المواعيد، والفحوصات المختبرية، والإجراءات التشخيصية والعلاجية، والأدوية، ورسالة التحويل، والتقارير الطبية، وإخطار الولادة، وإخطار الوفاة.

3 - أن تكون الطباعة بناء طلب المريض أو من ينوب عنه.

4 - أن تحتوي كل ورقة مطبوعة على الرمز التعريفي للمستخدم الذي قام بالطباعة.

5 - إلغاء صلاحية الطباعة للأشخاص غير المصرح لهم القيام بها.

6 - توفير أداة إلكترونية لتتبع طباعة البيانات والتأكد من أن الطباعة تمت وفق القواعد المعمول بها.

8.15: مشاركة البيانات الصحية، يجب على المؤسسة الصحية عند مشاركة سجلات البيانات الصحية الخاصة بها في السجل الصحي الوطني، الالتزام بالضوابط الأتية:

1 - إخطار المريض بمشاركة بياناته الصحية مع المؤسسات الصحية الأخرى من خلال السجل الصحي الوطني.

2 - استخدام الرقم المدني ورقم المقيم لتعريف (لتحديد هوية) المريض في السجل الصحي الوطني.

3 - توفير الأدوات التقنية اللازمة لربط السجلات الصحية للمؤسسة بالسجل الصحي الوطني.

4 - اقتصار مشاركة البيانات الصحية على الحد الأدنى من البيانات المطلوبة في السجل الصحي الوطني.

8.15.1: يجب على المؤسسة الصحية مشاركة بياناتها مع المؤسسات الصحية ذات العلاقة من خلال السجل الصحي الوطني لضمان التكامل الرقمي في الأنظمة.

8.15.2: يجب أن تكون مشاركة البيانات الصحية للمؤسسة الصحية من خلال السجل الصحي الوطني، وفقا للضوابط الآتية:

1 - أن تكون المشاركة لأغراض مشروعة فقط.

2 - أن يكون استخدام البيانات المشتركة وفقا لمبدأ الحاجة إلى المعرفة المبررة فقط

3 - خضوع البيانات الصحية لاتفاقيات مشاركة البيانات بين الجهات ذات العلاقة.

4 - مراعاة المخاطر المحتملة على صاحب البيانات عند تقييم أي طلب مشاركة بيانات

8.15.3: تكون مشاركة البيانات الصحية بين وحدات الجهاز الإداري للدولة وغيرها من الأشخاص الاعتبارية العامة وفقا للضوابط الآتية:

1 - أن يتم تقييم الفوائد والمخاطر المحتملة على الأفراد أو المجتمع من مشاركة البيانات أو عدم مشاركتها.

2 - الاحتفاظ بسجلات خاصة بالقرارات ذات الصلة بمشاركة البيانات وأسبابها، فإذا كان القرار يسمح بالمشاركة وجب توثيق أسباب المشاركة وأطرافها وأغراضها.

3 - التأكد من أن البيانات التي يتم مشاركتها ضرورية للغرض المحدد لها، ومع الأشخاص الذين يحتاجون إليها فقط، وأنها دقيقة ومحدثة، وأن تكون مشاركتها في الوقت المناسب، وبطريقة آمنة.

4 - تقييم ما إذا كانت هناك التزامات قانونية تجب مراعاتها قبل الدخول في اتفاقات بشأن مشاركة البيانات.

5 - الالتزام بقانون حماية البيانات الشخصية.

6 - عدم مشاركة البيانات مع طرف آخر أو جهة أخرى إلا بموافقة الجهة المالكة لتلك البيانات كجزء من اتفاقيات مشاركة البيانات.

7 - التأكد عند حفظ أو نقل البيانات الشخصية من تطبيق الإجراءات التقنية وغير التقنية المناسبة ذات الصلة بأمن المعلومات.

8 - تعزيز وعي الموظفين بقواعد وإجراءات مشاركة البيانات.

8.15.4: يجب على المؤسسة الصحية الالتزام بمبادئ جودة البيانات التي تتم مشاركتها، وذلك من حيث الدقة، والشرعية، والاتساق، ومناسبة توقيت جمعها، وإتاحتها للغرض الذي طلبت لأجله، وصلتها بالغرض المطلوب، واكتمالها، وذلك على النحو الآتي:

1 - أن تكون البيانات دقيقة وواضحة ومفصلة بشكل مناسب للأغراض المقصودة لها، ويجب تسجيلها مرة واحدة فقط، ولو كانت ستستخدم في أغراض متعددة.

2 - أن يتم تسجيل واستخدام البيانات بما يتفق والقوانين واللوائح ذات الصلة، بما يضمن تطابقها بين الجهات المختلفة عند مقارنتها خلال نفس الفترات الزمنية.

3 - أن تعكس البيانات دقة واتساق عملية جمعها من جميع النقاط خلال فترة زمنية معينة، وما إذا كانت الجهة تستخدم الجمع اليدوي أو أنظمة معتمدة على الكمبيوتر أو الطريقتين معا.

4 - أن تكون البيانات قد تم جمعها بأقصى سرعة ممكنة بعد الحدث أو النشاط، وإتاحتها للغرض الذي طلبت لأجله خلال فترة زمنية مناسبة، وذلك. بقدر كافٍ من السرعة والانتظام لأجل دعم الحاجات المعلوماتية وللمساهمة في تقديم الخدمات أو عملية اتخاذ القرارات المطلوبة.

5 - أن تكون البيانات المسجلة ذات صلة بالغرض الذي تستخدم لأجله، مع الالتزام بإجراء مراجعة دورية لمتطلباتها لتلبية الاحتياجات اللازمة للتغيير.

6 - أن تكون متطلبات البيانات قد تم تحديدها بوضوح بناءً على الاحتياجات المعلوماتية للجهة، والإجراءات الخاصة بجمعها ومدى موافقتها لتلك المتطلبات، مع الالتزام بمراقبة النقص وعدم الاكتمال والتسجيل غير الصحيح، كمؤشرات على جودة البيانات أو وجود بعض المشكلات في تسجيل عناصر بيانات محددة.

8.16: الإفصاح عن البيانات الصحية، يجوز للمؤسسة الصحية استخدام المعلومات الصحية للمريض أو تبادلها أو الإفصاح عنها لأغراض مختلفة، ومنها الآتي:

1 - العلاج وتقديم الخدمات الطبية المساعدة.

2 - التحصيل المالي.

3 - التعليم والتدريب.

4 - للأفراد المشاركين في رعاية المريض.

5 - لشركاء العمل.

6 - للتواصل مع المريض.

7 - لدليل المؤسسة الصحية.

8 - لاعتبارات الصحة والسلامة العامة.

9 - تنفيذا لأحكام القوانين والمراسيم السلطانية، أو لحكم أو أمر قضائي، أو تلبية لطلب جهة أمنية أو رقابية وفقا للقانون، أو بناء على طلب المريض أو من ينوب عنه للتحقيق في شكوى تتطلب الاطلاع على المعلومات الصحية للمريض.

10 - للتعويضات العمالية.

11 - للبحوث والدراسات.

12 - لمراجعة التوثيق والترميز الطبي.

8.16.1: الافصاح للعلاج والخدمات الطبية المساعدة، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لغرض تقديم العلاج والخدمات الطبية المساعدة له سواء في إطار تقديم وتنسيق وإدارة العلاج والرعاية الصحية والخدمات ذات الصلة، أو في إطار التواصل مع مؤسسات صحية في ذات الشأن، أو تنسيق الرعاية الصحية المنزلية وآلية إدارتها، وفقا للضوابط الآتية:

1 - اقتصار التصريح للفريق الطبي بالاطلاع على التاريخ المرضي للمريض، وعند الحاجة فقط.

2 - اقتصار التصريح للفريق الطبي في حالة الطوارئ الطبية (كسر الزجاج) بالاطلاع على الحد الأدنى للمعلومات الصحية فقط.

3 - عدم التصريح بالاطلاع على المعلومات الصحية للمريض لأسباب لا تخدم صحته أو سلامته.

8.16.2: الإفصاح للتحصيل المالي، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لغرض التحصيل المالي، وفقا للضوابط الآتية:

1 - أن يكون تبادل المعلومات والخطط العلاجية مقصورا على الدوائر المختصة والجهة المعنية بإدارة التأمين الصحي (منصة التأمين الصحي)، وشركات المطالبة، وشركات إدارة دورة الإيرادات، وشركات الترميز الطبي.

2 - أن يكون الإفصاح عن المعلومات قبل تلقى المريض الخدمات المقررة؛ لغرض الحصول على موافقة مسبقة، أو لمعرفة ما إذا كان التأمين سيغطي تكاليف العلاج من عدمه.

3 - أن تكون الجهة التي سيتم تبادل المعلومات معها خاضعة للقواعد الخاصة بتبادل المعلومات.

4 - أن يقتصر استخدام المعلومات المفصح عنها في نطاق العمل فقط.

5 - أن تلتزم جهات التحصيل المالي بقواعد الخصوصية والأمن المنصوص عليها في عقود الطرف الثالث وفقا للبند ١٠.٦ من هذه السياسة.

8.16.3: الإفصاح للتعليم والتدريب، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لطلبة كليات الطب والعلوم الصحية لأغراض التعليم والتدريب، وفقا للضوابط الآتية:

1 - أن يكون المتدرب تقدم بطب تدريب للتقسيم الإداري المختص بالتدريب.

2 - أن يكون التقسيم الإداري المختص بالتدريب قد وافق على طلب التدريب.

3 - أن يتم منح المتدرب بطاقة متدرب تتضمن تاريخ بدء وانتهاء التدريب.

4 - توقيع المتدرب على إقرار بالحفاظ على خصوصية وأمن البيانات خلال فترة التدريب.

5 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات بمنح الحد الأدنى من الصلاحيات للمتدرب للاطلاع على الحد الأدنى من البيانات الصحية لتلبية أهداف التدريب.

6 - أن يتم غلق حساب المتدرب في النظام تلقائيا بعد انقضاء فترة التدريب.

7 - التزام المتدرب بإعادة بطاقة المتدرب للتقسيم الإداري المختص بالتدريب فور الانتهاء من التدريب.

8.16.4: الإفصاح للأفراد المشاركين في رعاية المريض، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض للأفراد المشاركين في رعاية المريض في الحالات ووفقا للضوابط الآتية:

1 - أن يكون الإفصاح للجهات والأفراد المعنيين في الحالات الطارئة؛ لغرض الإبلاغ عن الموقع والوضع الصحي للمريض.

2 - أن يكون الإفصاح لأي من أقارب المريض حتى الدرجة الرابعة أو من ينوب عنه؛ لغرض الإبلاغ عن حالته الصحية، وذلك ما لم يكن المريض قد حدد أفرادا بذواتهم للإفصاح لهم، فعندئذ يجب قصر الإفصاح على هؤلاء الأشخاص دون غيرهم.

3 - أن يكون الإفصاح في حالة المريض عديم أو ناقص أو فاقد الأهلية لمن ينوب عنه؛ لغرض الإبلاغ عن حالته الصحية.

8.16.5: الإفصاح للشركاء العمل, يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لشركاء العمل وفقا للضوابط المحددة في البند (10.4) من هذه السياسة.

8.16.6: الإفصاح للتواصل مع المريض, يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض للتواصل معه، وفقا للضوابط الآتية:

1 - أن يكون الاتصال لغرض تحديد المواعيد، أو تقديم الإرشادات السريرية، أو إجراء المسوحات، أو غيرها من الإجراءات الطبية، ويحظر استخدام البيانات أو الإفصاح عنها خارج هذا النطاق.

2 - أن يكون الاتصال في وقت مناسب لظروف العمل وحالة المريض.

3 - أن يكون الاتصال من مكان يكفل حفظ خصوصية وسرية البيانات.

4 - التزام المتصل بالإفصاح للمريض عن اسمه واسم المؤسسة الصحية التابع لها.

5 - التزام المتصل بالتحقق من هوية متلقي الاتصال وصلة قرابته بالمريض قبل الإفصاح له عن سبب الاتصال.

6 - استخدام المتصل المفردات المناسبة بما يكفل احترام مشاعر وخصوصية المريض.

7 - التخلص من أي وثائق ورقية تم استخدامها في الاتصال تحتوي على بيانات المريض.

8.16.7: الإفصاح لدليل المستشفى، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لدليل المستشفى في حالة تنويمه فيها، وفقا للضوابط الآتية:

1 - أن يقتصر الإفصاح على المعلومات العامة، كاسم المريض، ومكان تنويمه.

2 - موافقة المريض أو من ينوب عنه قبل إدراج بياناته في دليل المستشفى.

8.16.8: الإفصاح للصحة والسلامة العامة، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية وتبادلها لأغراض الصحة والسلامة العامة، وفقا للضوابط الآتية:

1 - أن يكون الإفصاح والتبادل في حالة الضرورة فقط، كتفادي خطر يهدد صحة وسلامة المريض أو الصحة والسلامة العامة.

2 - أن يقتصر الإفصاح والتبادل على الجهات القادرة على المساعدة ومنع الخطر أو الحد منه.

3 - التزام الموظفين باتباع إجراءات وضوابط خصوصية وأمن المعلومات الصحية.

4 - أن يكون الإفصاح أو التبادل بسبب أو بمناسبة أي من الآتي:

أ- اتخاذ إجراءات الوقاية من مرض أو إصابة أو إعاقة ومكافحتها.

ب- الإبلاغ عن المواليد أو الوفيات.

ج- الإبلاغ عن إساءة معاملة الأطفال أو إهمالهم.

د- الإبلاغ عن الآثار الجانبية للأدوية أو المشاكل التي تسببها بعض المنتجات.

هـ -الإعلان عن سحب منتجات من التداول تشكل خطرا على الصحة أو السلامة العامة.

و- إخطار الشخص الذي تعرض لمرض أو كان عرضة لخطر الإصابة به، أو لنشر العدوى.

ح- إبلاغ وحدات الجهاز الإداري المختصة عن الاشتباه بتعرض مريض بالغ لسوء المعاملة أو الإهمال أو العنف المنزلي.

ط- تعزيز إجراءات وتدابير مراقبة الصحة العامة، ومكافحة الإرهاب البيولوجي.

ك- اتخاذ إجراءات الوقاية من الأمراض التي تهدد الصحة العامة.

8.16.9: الإفصاح لما يقتضي القانون، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية تنفيذا لحكم القانون في الحالات الآتية:

1 - بناء على طلب الجهات الأمنية، أو الجهات القضائية (الادعاء العام أو المحاكم)، أو المؤسسات الإصلاحية.

2 - بناء على طلب الجهات الرقابية.

3 - بناء على طلب المريض أو من ينوب عنه؛ للتحقيق في شكوى مقدمة منه للمؤسسة الصحية.

8.16.9.1: الإفصاح للجهات الأمنية أو الادعاء العام أو المحاكم أو المؤسسات الإصلاحية، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للجهات الأمنية، والجهات القضائية (الادعاء العام والمحاكم)، والمؤسسات الإصلاحية، وفقا للضوابط الآتية:

1 - ورود طلب لإدارة المؤسسة الصحية من الجهة الأمنية أو القضائية للإفصاح عن البيانات الصحية.

2 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات بمنح صلاحيات الوصول للجهة الأمنية أو القضائية، ويكون التصريح بالوصول للمعلومات في الحدود وبالقدر الذي تقتضيه حاجة العمل فقط.

3 - تأكد التقسيم الإداري المختص بإدارة المعلومات الصحية من توفير المعلومات المطلوبة كاملة بما فيها التعديل أو الحذف الوارد عليها.

4 - أن يكون منح صلاحيات الوصول للمعلومات وفقا لمعايير خصوصية وأمن المعلومات.

5 - التزام جهة التحقيق بإخطار التقسيم الإداري المختص بإدارة المعلومات الصحية فور انتهاء من التحقيق بما يفيد الانتهاء منه.

6 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بإلغاء صلاحيات الوصول للمعلومات الصحية فور إخطاره بانتهاء التحقيق.

7 - للتقسيم الإداري المختص بإدارة المعلومات الصحية - عند اللزوم - إرسال المعلومات عن طريق القنوات الرسمية للجهة مقدمة الطلب وبطريقة تضمن خصوصية وسرية المعلومات، بدلا عن التصريح لها بالوصول إليها.

8.16.9.2:الإفصاح بموجب طلب من الجهات الرقابية، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية لجهات التدقيق و الرقابية، وفقا للضوابط الآتية:

1 - ورود طلب لإدارة المؤسسة الصحية من الجهة الرقابية للإفصاح عن البيانات الصحية.

2 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات بمنح صلاحيات الوصول للجهة الرقابية، ويكون التصريح بالوصول للمعلومات في الحدود وبالقدر الذي تقتضيه حاجة العمل فقط.

3 - الالتزام في منح صلاحيات الوصول للمعلومات بمعايير خصوصية وأمن المعلومات.

4 - التأكد من أن المختصين في جهة التدقيق والرقابة قد اجتازوا برنامج تدريبي لمعرفة الاستخدام الصحيح لأنظمة المعلومات الصحية.

5 - التزام جهة التدقيق والرقابة بإخطار التقسيم الإداري المختص بإدارة المعلومات الصحية فور انتهاء من التدقيق بما يفيد الانتهاء منه.

6 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بإلغاء صلاحيات الوصول للمعلومات فور انتهاء التدقيق.

8.16.9.3: الإفصاح بموجب طلب من المريض أو ولية أو من ينوب عنة للتحقيق في شكوى تتطلب الاطلاع على معلومات المريض: يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية بناء على طلب المريض أو من ينوب عنه لجهة التحقيق في شكوى مقدمة منه للمؤسسة، وفقا للضوابط الآتية:

1 - ورود طلب للمؤسسة الصحية من المريض أو من ينوب عنه للإفصاح عن المعلومات الصحية لجهة التحقيق.

2 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات بمنح جهة التحقيق صلاحيات الوصول للمعلومات الصحية في الحدود وبالقدر اللازم لما تقتضيه الحاجة فقط.

3 - تأكد التقسيم الإداري المختص بإدارة المعلومات الصحية من توفير المعلومات المطلوبة كاملة بما فيها التعديل أو الحذف.

4 - التزام جهة التحقيق بإخطار التقسيم الإداري المختص بإدارة المعلومات الصحية فور الانتهاء من التحقيق بما يفيد الانتهاء منه.

5 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بإلغاء صلاحيات الوصول للمعلومات الصحية فور إخطاره بانتهاء التحقيق.

8.16.10: الإفصاح للتعويضات العمالية، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية في حالات المطالبات الوظيفية أو العمالية بالتعويض عن إصابات العمل، لجهات الاختصاص فقط، وبالقدر اللازم للفصل في تلك المطالبات.

8.16.11: الإفصاح للبحوث والدراسات، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لأغراض البحوث العلمية والدراسات، وفقا للضوابط الآتية:

1 - ورود طلب لإدارة المؤسسة الصحية من الجهة البحثية أو القائمة بالدراسة برغبتها أو حاجتها للوصول إلى المعلومات الصحية.

2 - أن يحدد في الطلب نوع وحجم المعلومات اللازمة لإجراء الدراسة أو المشروع البحثي.

3 - التزام التقسيم الإداري المختص بالمعلومات الصحية بتوفير البيانات المطلوبة أو إعطاء الجهة البحثية أو القائمة بالدراسة الصلاحيات اللازمة للوصول إليها بالحد الأدنى اللازم لإنجاز الدراسة أو المشروع البحثي.

4 - إخفاء هوية المريض (بياناته التعريفية) عند إجراء البحث أو الدراسة.

5 - أخذ موافقة المريض في حالة حاجة الجهة البحثية أو القائمة بالدراسة للاطلاع على معرفات المريض.

6 - التزام الجهة البحثية أو القائمة بالدراسة في الاطلاع بالمعلومات الصحية التي تخدم المشروع البحثي أو الدراسة دون غيرها.

7 - التزام الجهة البحثية أو القائمة بالدراسة بعدم نشر المعلومات الجينية والضخمة التي قد تشير لصاحبها أو توثر على سمعة الدولة.

8 - التزام الجهة البحثية أو القائمة بالدراسة بإخطار التقسيم الإداري المختص بإدارة المعلومات الصحية فور الانتهاء من الدراسة أو المشروع البحثي بما يفيد الانتهاء منه.

9 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بإلغاء صلاحيات الوصول للمعلومات الصحية فور انتهاء الجهة البحثية أو القائمة بالدراسة من الدراسة أو المشروع البحثي، أو من وقت إفصاحها قبل ذلك بالاكتفاء بما تم الاطلاع عليه.

8.16.12: الإفصاح لمراجعة التوثيق والترميز الطبي، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض لأغراض مراجعة التوثيق والترميز الطبي للأمراض والتدخلات الجراحية، للاستخدام من قبل المختصين فقط وفقا للقواعد الدولية المتبعة في هذا الشأن.

8.14.13: الإفصاح عن المعلومات في حالات خاصة، يجب أن يكون إفصاح المؤسسة الصحية عن المعلومات الصحية للمريض في حالات خاصة، وفقا للضوابط الآتية:

1 - ورود طلب لإدارة المؤسسة الصحية من قبل الجهة المعنية برغبتها أو حاجتها للوصول إلى المعلومات الصحية.

2 - أن يحدد في الطلب نوع وحجم البيانات اللازم الاطلاع عليها وسبب الاطلاع.

3 - إحالة الطلب بعد الموافقة عليه إلى للتقسيم الإداري المختص بالمعلومات الصحية للتنفيذ.

4 - التزام التقسيم الإداري المختص بالمعلومات الصحية بتوفير البيانات المطلوبة أو إعطاء الجهة المعنية الصلاحيات اللازمة للوصول إليها بالحد الأدنى اللازم لإنجاز عملها.

5 - إخفاء هوية المريض (بياناته التعريفية).

6 - أخذ موافقة المريض في حالة حاجة الجهة المعنية للاطلاع على هويته.

7 - التزام الجهة المعنية بإخطار التقسيم الإداري المختص بإدارة المعلومات الصحية فور الانتهاء من إنجاز عملها بما يفيد الانتهاء منه.

8 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بإلغاء صلاحيات الوصول للمعلومات الصحية فور انتهاء الجهة المعنية من انجاز عملها، أو من وقت إفصاحها قبل ذلك بالاكتفاء بما تم الاطلاع عليه.

8.17: إتاحة البيانات المفتوحة، يجب أن تكون إتاحة البيانات المفتوحة وفقا للقواعد والإجراءات الخاصة بالبيانات الحكومية المفتوحة الصادرة من وزارة النقل والاتصالات وتقنية المعلومات.

8.18: تجميد السجل الصحي بعد الوفاة، يجب على المؤسسة الصحية تجميد السجل الصحي للمريض بعد وفاته، وفقا للضوابط الآتية:

-1 توثيق بيانات المريض في حالة عدم وجود زيارة نشطة - عند الحاجة - وفقا للضوابط المنصوص عليها في البند 8.5.2 من هذه السياسة، خلال (10) عشرة أيام من تاريخ الوفاة.

-2 تجميد السجل الصحي للمريض عن أداء أي عمل إجرائي بعد مضي (10) عشرة أيام من تاريخ الوفاة.

-3 تجميد جميع سجلات المريض المتوفي على المستوى الوطني.

8.19: الاحتفاظ بالسجلات وأرشفتها وإتلافها، تلتزم المؤسسة الصحية باتباع قواعد حفظ وأرشفة وإتلاف السجلات الصحية الورقية والإلكترونية والأجهزة والمعدات وفقًا لجدول مدد استبقاء الوثائق المعتمد من هيئة الوثائق والمحفوظات الوطنية.

8.19.1: يجب أن يكون حفظ المؤسسة الصحية للسجلات الصحية وأرشفتها وفقا للضوابط الآتية:

1 - تصنيف جميع السجلات والاحتفاظ بها وفقًا لقانون الوثائق والمحفوظات ولائحته التنفيذية.

2 - تصنيف السجل الصحي كوثيقة جارية في حال استمرار المريض في العلاج.

3 - تصنيف السجل الصحي كوثيقة وسيطة في الحالات الآتية:

أ- بعد انقطاع المريض عن العلاج مدة تزيد على (10) عشر سنوات.

ب- بعد (10) عشر سنوات من تاريخ وفاة المريض.

4 - أرشفة السجل الصحي بعد انقضاء فترته كوثيقة وسيطة.

5 - يمكن للمؤسسة الصحية انتقاء مكونات محددة بالسجل الصحي للأرشفة بهدف التنظيم وتخفيف العبء على الخوادم. ويكون انتقاء المكونات حسب نوع وأهمية المكون مع الأخذ في الاعتبار العوامل الآتية:

أ- نوع المرض.

ب- سبب العلاج.

ج- نوع الزيارة (زيارات الترقيد، زيارات العيادات الخارجية، زيارات قسم الطوارئ، زيارات الرعاية النهارية).

6 - ضمان الاسترجاع السريع لأي بيانات من الأرشفة عند الحاجة إليها.

7 - توفير التقنيات والبرامج اللازمة للاسترداد وقراءة الوثائق التي تمت أرشفتها والتأكد من سلامتها عند الاسترداد.

8 - أرشفة جميع السجلات بطريقة آمنة تضمن سهولة تخزينها وفهرستها واستردادها.

9 - أن يوضح السجل الصحي عناوين المكونات التي تم نقلها للأرشفة.

10 - تسليم المؤسسة الصحية في حال إغلاقها جميع سجلاتها الصحية بكافة أنواعها للوزارة.

8.19.2: التخلص من الوسائط الخارجية /الأجهزة

8.19.2.1: التخلص من الوسائط الخارجية، يجب على المؤسسة الصحية عند إتلاف أو التخلص من الوسائط الخارجية كالأقراص المضغوطة وأقراص DVD ومحركات أقراص USB والأقراص الصلبة الخارجية وكذلك بطاقات SSD وغيرها من الوسائل المنقولة لتخزين البيانات التي تكون في حوزة الموظف ويحتمل أن تحتوي على معلومات سرية، ضمانا لعدم فقدان البيانات وعدم المساس بسريتها وأمانها، الالتزام بالضوابط الآتية:

1 - يتحمل الموظف مسؤولية تحديد وتسليم الوسائط الخارجية الواجب اتلافها أو التخلص منها وفقا للأحكام هذه السياسة.

2 - عدم إلقاء الوسائط الخارجية في المهملات مطلقا.

3 - إرسال الوسائط بجميع أشكالها - في حال عدم الحاجة إليها - إلى التقسيم الإداري المختص بتقنية المعلومات للتخلص منها بالشكل المناسب.

4 - التزام التقسيم الإداري المختص بتقنية المعلومات بتأمين الوسائط الخارجية حتى يتم التخلص منها بالطرق المناسبة وفقا لإرشادات هيئة الوثائق والمحفوظات الوطنية.

8.19.2.2: التخلص من الوسائط المعدات/ الأجهزة، يجب على المؤسسة الصحية عند التخلص من أجهزة الحاسب الآلي مراعاة الضوابط الآتية:

1 - التأكد من مسح جميع البيانات من تلك الأجهزة.

2 - إعادة إعدادات تلك الأجهزة إلى حالة إعدادات المصنع الافتراضية.

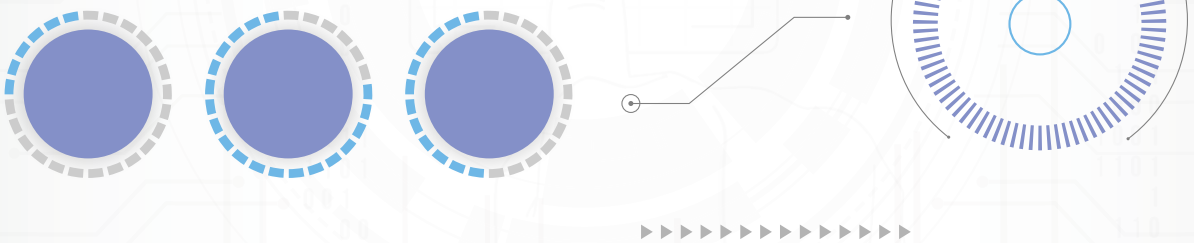
3 - عدم إجراء أي إعدادات أو تكوينات أو تثبيت أي برامج أو تطبيقات في تلك الأجهزة

4 - عند استبدال أجهزة جديدة بالأجهزة القديمة، يتم الاحتفاظ بالأخيرة ضمن المخزون لاستخدامها عند الحاجة كقطع غيار، أو في حالات الطوارئ، أو لاختبار البرامج الجديدة، أو كنسخ احتياطية.

5 - إصدار شهادة تكهين لكل معدة أو جهاز قديم غير صالح للعمل بعد استبداله.

6 - إتلاف القرص الصلب في الجهاز بعد تكهينه وقبل إرساله إلى التقسيم الإداري المختص للتصرف فيه بالبيع.

7 - التخلص من كافة الأجهزة بحسب الإجراءات المتبعة من قبل الهيئة الوطنية للوثائق والمحفوظات.



الفصـــــــل الخامس

9. حقوق الشخص على ملفه الصحي

9 حقوق الشخص على ملفه الصحي:

9.1: تعد البيانات الشخصية في الأنظمة الصحية ملكا للدولة، وتلتزم المؤسسة الصحية بمعالجتها في إطار من الشفافية، والأمانة، واحترام كرامة الإنسان، وبعد موافقة مكتوبة وواضحة وصريحة ومفهومة من صاحبها.

9.2: يحق للمريض الحصول على نسخة من معلوماته الصحية (ملخص الترخيص والفحوصات المختبرية، وقائمة الأدوية، والإجراءات التشخيصية والعلاجية وسجل التحصينات)، ويجب على التقسيم الإداري المختص بإدارة المعلومات الصحية تلبية طلبه في هذا الشأن.

9.3: يحق للمريض الحصول على تقرير طبي مفصل عن حالته الصحية وفقا للضوابط الآتية:

1 - ورود طلب من المريض أو ممن ينوب عنه إلى التقسيم الإداري المختص بإدارة المعلومات الصحية للحصول على تقرير طبي مفصل عن حالته الصحية.

2 - سداد الرسوم المقررة للطلب إن وجدت.

3 - البت في الطلب وتسليم التقرير الطبي لمقدمه خلال (15) خمسة عشر يوم عمل من تاريخ تقديمه.

4 - في حالة رفض الطلب يجب أن يكون القرار مسببا مع إخطار مقدمه بالأسباب.

9.4: يحق للمريض طلب إجراء تعديل على بياناته الصحية، ويشمل ذلك محو البيانات غير الصحيحة.

9.5: يجب أن يكون تعديل البيانات الصحية للمريض، وفقا للضوابط الآتية:

1 - ورود طلب من المريض أو ممن ينوب عنه إلى التقسيم الإداري المختص بإدارة المعلومات الصحية لتعديل بياناته الصحية.

2 - سداد الرسوم المقررة للطلب إن وجدت

3 - البت في الطلب وإجراء التعديل خلال (15) خمسة عشر يوم عمل من تاريخ تقديمه.

4 - في حالة رفض الطلب يجب أن يكون القرار مسببا مع إخطار مقدمه بالأسباب.

9.6: يجب أن يكون رفض تعديل البيانات الصحية بناء على طلب المريض لأحد الأسباب الآتية:

1 - إذا لم تقم المؤسسة الصحية بإنشاء البيانات الصحية، أو صارا من قام بإنشائها غير متاح لإجراء التعديل.

2 - ثبوت صحة واكتمال البيانات الصحية المسجلة.

3 - أن تكون البيانات المراد تصحيحها ليست جزءا من البيانات الصحية التي يجوز للمريض فحصها أو طلب تعديلها.

9.7: يحق للمريض طلب تعديل بياناته الديموغرافية من خلال موظف التسجيل في المؤسسة الصحية مباشرة بمجرد إبراز البطاقة المدنية دون حاجة إلى تقديم طلب أو اتخاذ إجراء آخر.

9.8: يحق للمريض الحصول على قائمة عمليات الإفصاح عن بياناته الصحية، وفقا للضوابط الآتية:

1 - ورود طلب من المريض أو ممن ينوب عنه إلى التقسيم الإداري المختص بإدارة المعلومات الصحية للحصول على قائمة الإفصاح.

2 - سداد الرسوم المقررة للطلب إن وجدت.

3 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بحصر عمليات الإفصاح لمدة لا تتجاوز عام ميلادي سابق على تاريخ تقديم الطلب.

4 - البت في الطلب وتسليم مقدمه قائمة الإفصاح خلال (15) خمسة عشر يوما من تاريخ تقديم الطلب.

5 - تضمين قائمة الإفصاح تاريخ الإفصاح، والجهة المفصح لها، ونوع المعلومات المفصح عنها، وأسباب الإفصاح.

9.9: استثناء من حكم البند ٩.٨ من هذه السياسة، لا يجوز أن تتضمن قائمة الإفصاح الواجب تسليمها للمريض أو من ينوب عنه قانونا البيانات الآتية:

1- المعلومات المستخدمة لأغراض تقديم الرعاية الصحية أو سداد التكاليف.

2 - المعلومات التي تم الإفصاح عنه بطلب من المريض أو بموافقته.

3 - المعلومات التي تم تقديمها للأفراد المعنيين بتقديم الرعاية للمريض إما بهدف الإخطار والتوجيه، أو لأغراض الإغاثة في حالات الكوارث.

4 - المعلومات التي تم تقديمها تنفيذا لحكم أو قرار قضائي أو لجهة أمنية بناء على طلبها وفقا للقوانين المعمول بها.

5 - المعلومات التي تم تقديمها إلى المؤسسات الإصلاحية أو الموظفين المسؤولين عن إنفاذ القانون.

6 - المعلومات التي تم استخدامها كجزء من مجموعة بيانات محدودة لا تحتوي على معلومات صحية معينة من شأنها أن تحدد هوية المريض.

7 - البيانات الصحية المتعلقة بتوظيف الفرد أو تجديد عقود الخدمة.

9.10: يحق للمريض - في حال رغبته تغيير المؤسسة الصحية أو الطبيب المعالج - نقل بياناته الصحية إلى متحكم آخر من خلال التقسيم الإداري المختص بإدارة البيانات الصحية وفق إحدى الطريقتين الآتيتين:

1- طلب الحصول على نسخة من بياناته الصحية لمتابعة العلاج مع مؤسسة صحية أخرى.

2 - طلب تحويل بياناته الصحية لطبيب معالج آخر داخل المؤسسة الصحية ذاتها.

9.11: يحق للمريض طلب حجب بياناته الصحية أو فرض قيود للحد من استخدامها والإفصاح عنها بما في ذلك مشاركتها في السجل الصحي الوطني، وذلك وفقا للضوابط الآتية:

1- ورود طلب من المريض أو ممن ينوب عنه إلى التقسيم الإداري المختص بإدارة المعلومات الصحية لحجب بياناته الصحية أو فرض قيود للحد من استخدامها والإفصاح عنها.

2 - سداد الرسوم المقررة إن وجدت.

3 - يجب فحص الطلب والبت فيه وإخطار مقدمه بالقرار خلال (15) خمسة عشر يوما من تاريخ تقديمه.

4 - في حالة رفض الطلب يجب أن يكون القرار مسببا، وإخطار مقدم الطلب بأسباب الرفض.

9.12: يستثنى من حكم البند ٩.١١ من هذه السياسة، الإفصاح عن المعلومات الصحية للمريض في الحالات الآتية:

1 - العلاج في حالات الطوارئ.

2 - الاستخدامات التي لا تستدعي الحصول على إذن شخصي مسبق من المريض.

3 - تنفيذا لحكم أو أمر قضائي أو بناء على طلب الجهات الأمنية وفقا للقانون.

9.13: يجب على التقسيم الإداري المختص بإدارة المعلومات الصحية إخطار المريض كحق من حقوقه بأي اختراق وانتهاك يحدث لبياناته الصحية، وفقا للضوابط الآتية:

1 - أن يتم الإخطار خلال (10) عشرة أيام عمل من تاريخ الاختراق أو الانتهاك.

2 - أن يشمل الإخطار كافة الانتهاكات أو الاختراقات التي حدثت على بياناته الصحية.

3 -أن يتضمن الإخطار بيان طبيعة البيانات التي تم اختراقها أو انتهاكها.

4 - أن يتضمن الإخطار بيانا بالإجراءات التي تم اتخاذها أو سيتم اتخاذها للحد من آثار الاختراق أو الانتهاك.

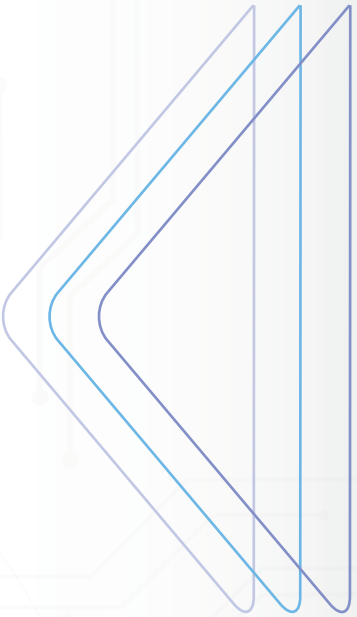
5 - أن يتضمن الإخطار تحديد نقطة اتصال يمكن للمريض الرجوع إليها في حالة وجود استفسار لديه بخصوص الاختراق أو الانتهاك.

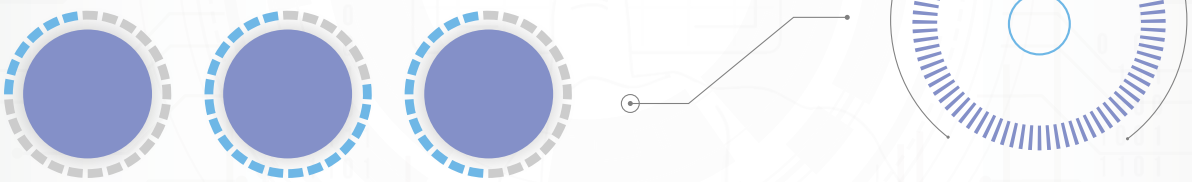
9.14: يحق للمريض - في حالة عدم توافق معالجة بياناته الصحية مع أحكام قانون حماية البيانات الشخصية ولائحته التنفيذية - التقدم بشكوى للمؤسسة الصحية وفقا للضوابط الآتية:

1 - أن تقدم الشكوى من المريض أو ممن ينوب عنه إلى التقسيم الإداري المختص في المؤسسة الصحية.

2 - فحص الشكوى والبت فيها وإخطار مقدمها بالقرار خلال (15) خمسة عشر يوم عمل من تاريخ تقديمها، ويعتبر مضي هذا الميعاد دون البت فيها قرارا بالرفض.

3 - يحق للمريض التظلم إلى من قرار الرفض إلى إدارة المؤسسة الصحية خلال (15) خمسة عشر يوما من تاريخ إخطاره بقرار الرفض أو من تاريخ مضي (15) خمسة عشر يوما على تقديم الشكوى دون البت فيها.





الفصـــــــل السادس

10. الاتصال بالشبكة

11. المخاطر البرمجية

12. استخدام أنظمة الذكاء الاصطناعي

13. الحوسبة السحابية

14. تشفير البيانات

15. إدارة تحديث الأنظمة

16. عمليات التدقيق

17. مراجعة نشاط نظم المعلومات

18. سلامة البيانات

10 الاتصال بالشبكة:

10.1: يجب في حال الاتصال بشبكة المؤسسة الصحية من خارجها سواء بسبب التصريح للموظف بالعمل عن بعد، أو للاتصال بموقع طرف ثالث، أو بسبب عقود تم إبرامها مع طرف ثالث، مراعاة الأحكام البنود الواردة التالية.

10.2: يجب على المؤسسة الصحية في حال الترخيص للموظف بالعمل عن بعد استيفاء المتطلبات العامة لقواعد خصوصية وأمن المعلومات، على النحو الآتي:

1 - منح الموظف تصريح للعمل عند بعد من التقسيم الإداري المختص بإدارة المعلومات الصحية، بناء على طلب من رئيسه المباشر.

2 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بتوفير الإجراءات اللازمة للعمل عن بعد بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات.

3 - تعهد الموظف المصرح له بالعمل عن بعد بالالتزام بضوابط وإجراءات الخصوصية والأمن.

4 - التأكد من تزويد الموظف المصرح له بالعمل عن بعد بإمكانية الوصول إلى المعرفة بالقدر اللازم لإنجاز المهام المطلوبة.

5 - تحديد الوصول عن بعد إلى الحد الأدنى من الموارد المطلوبة لإنجاز المهام.

6 -التزام الموظف المصرح له بالعمل عن بعد باستعمال كلمة مرور قوية مستوفاة للمعايير المنصوص عليها في هذه السياسة.

7 - إكمال الموظفين المصرح لهم بالعمل عن بعد لبرنامج التدريب السنوي على الخصوصية والأمن، كأقرانهم من الموظفين في بيئة العمل التقليدية، ويتولى مسؤولية تنفيذ هذا التدريب كل من: التقسيم الإداري المختصة بإدارة المعلومات الصحية والتقسيم الإداري المختص بتقنية المعلومات.

8 - التزام الموظف بعدم استخدام الجهاز المعد للعمل عن بعد في الاستخدامات الشخصية.

9 - التزام الموظف باتخاذ الإجراءات الكفيلة بحماية الجهاز المعد للعمل عن بعد من السرقة أو الفقد أو الأضرار المادية.

10 - تأكد الموظف من عمل كافة التحديثات اللازمة بأجهزة العمل عن بعد بما فيها التحديثات الأمنية.

11 - التزام الموظف المصرح له بالعمل عن بعد باستخدام البرامج الموثوقة والمرخصة من قبل المؤسسة فقط.

12 - تأكد التقسيم الإداري المختص بتقنية المعلومات من توافق جهاز العمل عن بعد مع المعايير الأمنية للمؤسسة قبل تسليمه للموظف.

10.3: يجب على المؤسسة الصحية توفير الحماية الأمنية لأجهزة الحاسبات الآلية التي يستخدمها الموظف في حال التصريح له بالعمل عن بعد، وفقا للضوابط الآتية:

1 - تحديد نطاق شبكة آمن وموثوق للاتصال بشبكات المؤسسة، والتأكد من مطابقة الشبكات العامة للمواصفات الأمنية قبل الاستخدام.

2 - حظر مواقع الإنترنت غير المرتبطة بالعمل.

3 - تحمل كل تقسيم إداري في المؤسسة الصحية المسؤولية عما ينشئه من مواقع أو صفحات وما تحتويه من معلومات.

4 - تثبيت برنامج حماية من الفيروسات على جميع أجهزة الحاسبات الآلية، والعمل على تحديثها يوميا وبشكل آلي.

5 - اتباع الإجراءات المحددة عند الوصول إلى المعلومات في حال تطلب الأمر استخدام برنامج VPN وجدران الحماية.

6 - استخدام قفل الشاشة قبل الابتعاد عن مكان العمل، والتأكد من ضبط ميزة القفل التلقائي بعد (15) خمسة عشر دقيقة من عدم النشاط.

7 - توفير بيئة مكتبية آمنة معزولة عن الزوار والعائلة.

8 - تشفير البيانات واستخدام أحدث البروتوكولات في النقل والتصفح.

9 - استخدام كلمات مرور عالية الصعوبة مكونة من (8) ثمانية رموز على الأقل.

10 - ملاءمة استخدام حماية للشاشة للحد من سرقة البيانات عن طريق النظر.

11 - التأكد من تحديث نظام التشغيل بشكل دوري.

10.4: يجب على المؤسسة الصحية توفير حماية أمن البيانات في حال التصريح للموظف بالعمل عن بعد، وفقا للضوابط الآتية:

1 - التأكد من عمل نسخ احتياطي للبيانات باستمرار في وسائط تخزين خارجية.

2 - تشفير الأجهزة المستخدمة في العمل عن بعد بشكل صحيح ومناسب.

3 - تحديد فترة محددة للمستخدمين للاتصال بالشبكة.

4 - نقل البيانات إلى المؤسسة الصحية باستخدام اتصال VPN معتمد لضمان سرية وسلامة البيانات التي يتم إرسالها، وعدم التحايل على الإجراءات المعمول بها، وعدم إنشاء طريقة خاصة عند نقل البيانات إلى المؤسسة.

5 - توخي الحذر الشديد عند توصيل معدات التدريب بشبكة منزل أو فندق، لعدم قدرة المؤسسة الصحية على التحكم في الإجراءات الأمنية على الشبكات غير المملوكة لها.

6 - التأكد من منح الصلاحيات المناسبة مع قائمة التحكم في الوصول الممنوحة لكل مستخدم.

7 - التزام الموظف بإغلاق جميع السجلات الورقية في خزانة السجلات عند مغادرته منطقة عمله.

8 - التزام الموظف بعدم القيام بمهام العمل التي تتطلب استخدام معلومات حساسة على مستوى المؤسسة الصحية أو المريض في الأماكن العامة حيث يمكن للآخرين مشاهدة شاشة الكمبيوتر بسهولة من جانبه أو خلفه كالمطارات والطائرات وردهات الفنادق.

9 - أن تكون جميع عمليات النقل الخارجية للبيانات مرتبطة بعقد رسمي، أو اتفاقية عدم إفشاء، أو اتفاقية شراكة أعمال.

10 - حظر إعطاء أو نقل أي معلومات تخص المريض إلى أي شخص غير مصرح له.

11 - عدم الدخول من شبكة خارجية إلا بعد الحصول على موافقة مسبقة.

12 - تخويل التقسيم الإداري المختص بتقنية المعلومات الحق في إنهاء أي جلسة دخول غير مصرح به، دون إشعار مسبق.

10.5: يجب على التقسيم الإداري المختص بتقنية المعلومات في المؤسسة الصحية في حال الاتصال بموقع طرف ثالث إجراء تحليل للمخاطر بالتنسيق مع التقسيم الإداري المختص بإدارة المعلومات الصحية، يراعى في إجرائه الآتي:

1 - نوع الوصول المطلوب.

2 - قيمة المعلومات التي سيتم تداولها.

3 - التدابير الأمنية التي يستخدمها الطرف الثالث.

4 - الآثار المترتبة على أمن أنظمة المؤسسة الصحية.

10.6: لا يجوز للمؤسسة الصحية - في حال إبرام اتفاقيات عمل مع طرف ثالث - منح تصريح الوصول إلى أنظمة المؤسسة أو شبكات الشركات إلا بعد الانتهاء من مراجعة بنود اتفاقية العمل للتأكد من مراعاتها أو تضمينها أو ضمانها الآتي:

1 - معايير خصوصية وأمن المعلومات وتطبيقها.

2 - تقييم مخاطر الالتزامات الإضافية لكل طرف من أطراف الاتفاقية.

3 - الحق في مراجعة المسؤوليات التعاقدية.

4 - ترتيبات الإبلاغ عن الحوادث الأمنية والتحقيق.

5 - وصف لكل خدمة يتم إتاحتها.

6 - قصر مستوى الوصول للأنظمة والمعلومات على الحد الأدنى الضروري للطرف الثالث لأداء التزاماته التعاقدية.

7 - إعداد قائمة مفصلة بالمستخدمين الذين يمكنهم الوصول إلى أنظمة المؤسسة وقابليتها للتدقيق.

8 - حصر هوية وعدد موظفي الطرف الثالث الذين سيدخلون المؤسسة.

9 - تحديد المدة والفترات الزمنية التي تكون فيها الخدمة متاحة.

10 - الإجراءات المتعلقة بحماية موارد المعلومات وطريقة التدقيق.

11 - الحق في مراقبة وإلغاء نشاط المستخدم من قبل المؤسسة في كل اتفاقية.

12 - القيود المفروضة على نسخ المعلومات والكشف عنها في جميع الاتفاقيات.

13 - المسؤوليات المتعلقة بتثبيت الأجهزة والبرامج وصيانتها والاتفاق عليها مسبقًا.

14 - تدابير ضمان تدمير البرامج والمعلومات الموجودة لدى الشركة المتعاقدة في نهاية العقد.

15 - تدابير الحماية المادية الضرورية.

16 - إجراء برنامج تدريبي، وتحديد من يجب عليه تلقى التدريب ومن سيديره، وإنشاء محتوى التدريب

17 - نشر قائمة مفصلة بالإجراءات الأمنية التي سيتم اتخاذها من قبل جميع الأطراف قبل التوقيع على الاتفاقية.

11 المخاطر البرمجية:

11.1: يجب على المؤسسة الصحية تثبيت برنامج مكافحة الفيروسات على جميع الأجهزة المكتبية والمحمولة والكفية والخوادم المتصلة بموارد شبكة الحاسب الآلي التابعة للمؤسسة الصحية، بمراعاة الالتزام الآتي:

1 - التأكد من تحديث أنماط الفيروسات يوميا وبشكل آلي على الخوادم وأجهزة الحاسب الآلي.
2 - الاحتفاظ بسجل أنماط الفيروسات لجميع محطات العمل والخوادم على شبكة المؤسسة الصحية.

3- التأكد من وجود نظام مضاد للفيروسات في كل الأنظمة داخل المؤسسة الصحية.

4 - إخطار المختصين في حالة الكشف على فيروسات أو ملفات ضارة.

5 - على التقسيم الإداري المختص بتقنية المعلومات تقديم تقارير تدقيق دورية بشأن الفيروسات للجهات المختصة.

11.2: يحوز للمؤسسة الصحية الاستفادة في العمل من البرامج المشتركة والمفتوحة المصدر، وذلك بعد موافقة التقسيم الإداري المختص بتقنية المعلومات واتخاذ الاحتياطات الأمنية اللازمة قبل تثبيتها على أجهزة الحاسب الآلي والشبكات بما يضمن عدم احتوائها على فيروسات أو تداخلها على نحو يؤدي إلى تلف أجهزة أو برامج أو بيانات المؤسسة الصحية، وذلك وفقا للآتي:

1 - استخدام البرامج التي تم اعتمادها من قبل المختصين في مجال تقنية المعلومات فقط.

2 - اختبار جميع البرامج الجديدة من قبل المختصين في مجال تقنية المعلومات لضمان التوافق مع البرامج المثبتة وإعدادات الشبكة.

3 - قيام التقسيم الإداري المختص بتقنية المعلومات بفحص جميع البرامج بحثا عن الفيروسات قبل التثبيت، ويشمل ذلك البرامج التي يتم شراؤها مباشرة من المصادر التجارية والبرامج المشتركة والمفتوحة المصدر.

4 - فحص الأقراص المرنة والأقراص المضغوطة، وأقراص DVD، وأجهزة USB، قبل نسخ المعلومات منها إلى جهاز الحاسب الآلي.

5 - حظر إجراء عملية إعداد «installing » لأجهزة الحاسب الآلي من قرص مرن أو قرص مضغوط أو قرص DVD أو جهاز USB يتم استلامه من مصدر خارجي غير مصرح.

6 - حظر إجراء عملية تمهيد «booting» للحاسب الآلي من قرص مرن أو قرص مضغوط أو جهازUSP تم جلبه من مصدر خارجي غير مصرح.

7 - إزالة أي قرص أو جهاز متصل بجهاز الحاسب الآلي في حالة عدم استخدامه لضمان عدم وجودة عند بدء التشغيل؛ وذلك تجنبا للأضرار مثل نقل الفيروسات.

11.3: تكون البرامج والوثائق التي تم إنشاؤها أو توفيرها من قبل الموظفين في المؤسسة الصحية أو المتعاقدين معها ملكا للمؤسسة، وذلك ما لم تكن مشمولة باتفاق تعاقدي، ويجب على مطور البرامج أو الوثائق عند تعيينه التوقيع على إقرار بملكية المؤسسة الصحية للبرامج وفق اتفاقية الحفاظ على السرية.

11.4: يجب المؤسسة الصحية الالتزام بتصاريح الأنظمة والبرامج عند استخدامها، وإذا كان الترخيص لعدة مستخدمين فيجب عدم تجاوز العدد المصرح به من النسخ.

12 استخدام أنظمة الذكاء الاصطناعي:

12.1: يجوز للمؤسسة الصحية استخدام أنظمة الذكاء الاصطناعي في مجالات التشخيص، والمساهمة في تحسين الخطط العلاجية، وتطوير الأدوية، ومراقبة المريض ورعايته، وفي مجال الطب الشخصي

الموجه، كما يجوز لها استخدام خوارزميات الذكاء الاصطناعي لتحليل كميات كبيرة من البيانات بالاعتماد على السجلات الصحية الإلكترونية؛ للوقاية من الأمراض وتشخيصها.

12.2: يجب على المؤسسة الصحية في حال استخدامها أنظمة الذكاء الاصطناعي الالتزام بالآتي:

1 - الضوابط والمعايير والشروط المعتمدة من الجهات المختصة، والتي تتعلق بكل من: تصنيف البيانات، وحماية البيانات الشخصية، وأمن المعلومات والبيانات المفتوحة، واستمرارية الأعمال.
2 - التشريعات العمانية والاتفاقيات الإقليمية والدولية ذات الصلة بحقوق الإنسان.

3 - وضع الضوابط والمعايير والإجراءات الداخلية لتنظيم استخدام أنظمة الذكاء الاصطناعي.

4 - تحديد وتوثيق والاختصاصات والمسؤوليات ومستوى السلطة الإدارية ذات الصلة، وذلك خلال جميع مراحل تطوير أنظمة الذكاء الاصطناعي.

5 - توفير خصائص النفاذ الرقمي في أنظمة الذكاء الاصطناعي للأشخاص ذوي الإعاقة.

6 - إجراء تقييم لمخاطر أنظمة الذكاء الاصطناعي (الأمنية، والمالية والصحية، والبيئية) مع اتخاذ جميع التدابير الوقائية لمنع حدوث الأضرار المحتملة.

7 - توفير الموارد المطلوبة لحماية أنظمة الذكاء الاصطناعي من الهجمات السيبرانية، كالقرصنة وتسريب البيانات أو التلاعب بالخوارزميات وغيرها من الهجمات.

8 - التأكد من خلو خوارزميات أنظمة الذكاء الاصطناعي من التميز والانحياز لفئة معينة دون أخرى خلال جميع مراحل برمجتها وتدريبها.

9 - وضع آلية للتدقيق الداخلي على كافة الوسائل المستخدمة لجمع ومعالجة البيانات وبرمجة الخوارزميات وعمليات صنع القرارات المدعومة بالذكاء الاصطناعي.

10 - التدقيق والتحقق المستمر من جودة البيانات التي يتم تغذيتها في أنظمة الذكاء الاصطناعي بما يحقق النتائج الدقيقة ذات الجودة العالية.

11 - العمل على تصنيف أنواع القرارات (المؤتمتة والغير مؤتمتة) المعززة بالذكاء الاصطناعي.

12 - تحديد مستوى مناسب من التدخل البشري المطلوب لاتخاذ القرارات غير المؤتمتة، وعدم السماح لأنظمة الذكاء الاصطناعي باتخاذ القرارات الهامة بالنيابة عن الأشخاص المعنيين دون الحصول على تصريح مسبق منهم أو من المسؤولين عنهم قانونا.

13 - ضمان القدرة على تفسير قرارات أنظمة الذكاء الاصطناعي (المؤتمتة وغير المؤتمتة)، وذلك من خلال تتبع جذورها وسهولة الوصول إلى العوامل السببية خلفها.

14 - وضع أنظمة الذكاء الاصطناعي في بيئة اختبارية لفترات زمنية محددة لإجراء التجارب واختبار مدى فعاليتها وخلوها من الأخطاء قبل وضعها في البيئة التشغيلية.

15 - رصد وتسجيل جميع أنشطة الذكاء الاصطناعي في البيئة التشغيلية وعدم تركها دون رقابة.

16 - الإفصاح عن وجود أنظمة تعمل بالذكاء الاصطناعي في البيئة التشغيلية لجميع المتأثرين أو الجهات المسؤولة عنهم مع توضيح مدى تأثيرها عليهم.

17 - طلب الموافقة المسبقة من جميع المتأثرين أو المسؤولين عنهم قانونا في حال وجود قرارات مؤتمتة هامة تعمل بأنظمة الذكاء الاصطناعي وتؤثر عليهم تأثيرا مباشرا.

18 - وضع معايير لقياس مستوى جودة الخدمات المقدمة من خلال أنظمة الذكاء الاصطناعي.

19 - إعداد وتنفيذ خطة لاستمرارية خدمات أنظمة الذكاء الاصطناعي، مع توثيق الاختصاصات والمسؤوليات ومستوى السلطة الإدارية ذات الصلة.

13 الحوسبة السحابية:

13.1: يجوز للمؤسسة الصحية الاستفادة من خدمات الحوسبة السحابية، كخدمات البنية الأساسية، وخدمات المنصة، وخدمات البرمجيات.

13.2: يجب على المؤسسة الصحية في حال تبنيها مشروع يتطلب استخدام الخدمات السحابية مراعاة الضوابط والإجراءات ذات الصلة الصادرة من الجهات المختصة.

13.3: يجب على المؤسسة الصحية في حال استخدامها الخدمات السحابية استيفاء المتطلبات الآتية:

1 - متطلبات تصنيف البيانات.

2 - المتطلبات الأمنية.

3 - المتطلبات الإدارية.

4 - متطلبات استضافة البيانات والتطبيقات خارج سلطنة عمان.

13.4: يجب على المؤسسة الصحية في سبيل استيفاء متطلبات تصنيف البيانات لغرض استخدام الخدمات السحابية، الالتزام بالآتي:

1 - تحديد وبناء مجموعة البيانات الداخلية والخارجية.

2 - إنشاء سياسة داخلية لتصنيف البيانات وفقا للمراسيم السلطانية ذات العلاقة.

3 - إضافة مستوى خامس للبيانات المفتوحة أو المتاحة في السياسة الداخلية لاستيفاء متطلبات سياسة البيانات الحكومية المفتوحة.

4 - دراسة وتحليل المخاطر المتعلقة بالبيانات وتعيين متطلبات الحماية الأمنية اللازمة لها.

5 - الالتزام بقوانين وسياسات خصوصية وأمن البيانات المعمول بها في سلطنة عمان.

6 - الالتزام بالسياسات والمعايير والإرشادات الصادرة من مركز الدفاع الإلكتروني.

13.5: يجب على المؤسسة الصحية في سبيل استيفاء المتطلبات الأمنية لغرض استخدام الخدمات السحابية، الالتزام بالآتي:

1 - إجراء تقييم وإدارة المخاطر، وإعادة إجراء التقييم بشكل دوري على فترات تحددها المؤسسة، وذلك بالرجوع إلى إطار حوكمة الحوسبة السحابية.

2 - التقيد بالتشريعات ذات الصلة المرتبطة بإدارة المعلومات، بما في ذلك القضايا القانونية المتعلقة بالخصوصية وإدارة السجلات، وأي متطلبات أخرى قابلة للتطبيق كحقوق النشر والملكية والموقع الجغرافي للبيانات.

3 - التقيد بقوانين وأنظمة الدولة والسياسات والمعايير ذات الصلة التي تصدرها وزارة النقل والاتصالات وتقنية المعلومات أو مركز الدفاع الإلكتروني.

4 - تشفير البيانات والمعلومات المستضافة والمتداولة والمعالجة على البنية الأساسية القائمة على الحوسبة السحابية.

5 - عدم استضافة البيانات الصحية أو معالجتها في خدمات الحوسبة السحابية، ما لم يكن ذلك

تنفيذا لتدابير الأمن والخصوصية ومراقبتها، وذلك لحماية البيانات على النحو المحدد والمدعوم بنتائج تقييم المخاطر وتصنيف البيانات والالتزامات التعاقدية.

13.6: يجب على المؤسسة الصحية في سبيل استيفاء المتطلبات الإدارية لغرض استخدام الخدمات السحابية، الالتزام بالآتي:

1 - الاستعانة بمزودي الخدمة المعتمدين من وزارة النقل والاتصالات وتقنية المعلومات دون غيرهم.

2 - عدم تخزين البيانات والمعلومات الصحية في خوادم خارجية لا تربطها اتفاقيات تعاقدية سارية مع مزود الخدمة.

3 - اعتبار البيانات والمعلومات الصحية التي يتم استضافتها أو التعامل معها أو معالجتها على البنية الأساسية السحابية أصولا استراتيجية لوحدات الجهاز الإداري للدولة، وتتطلب إبرام اتفاقيات تعاقدية مع مزودي الخدمة للعمل بمقتضاها.

4 - التأكد من استيفاء مزود الخدمة متطلبات المعيار الدولي PCI DSS عند التعاقد معه، وذلك في حال تعامل المؤسسة بالتحويلات البنكية عبر الإنترنت.

5 - اتخاذ التدابير التعاقدية المناسبة عند التعاقد مع مزودي الخدمات (خدمات الحوسبة السحابية) لضمان الآتي:

أ- حماية البيانات الصحية، وعدم السماح لمزودي الخدمات المتعاقدين (وأي مقاولين ثانويين) بارتكاب أي أفعال أو ممارسات من شأنها انتهاك خصوصية المعلومات وأمنها، سواء كان مقدم الخدمة (وأي مقاول ثانوي) مقيما في سلطنة عمان، أو خارجها (في حالة منح استثناءات للخارج).

ب- سهولة إنهاء العقد أو نقل الخدمات في حالة انتقال المشروع إلى مزود جديد لخدمات الحوسبة السحابية.

ج- استرجاع جميع البيانات بالصيغ المعتمدة من قبل المؤسسة الصحية، في حالة إنهاء العقد.

6 - التأكد من قدرتها على تنفيذ بنود الاتفاقية، حتى عند التعاقد في الخارج.

7 - إعداد قائمة مرجعية للمساعدة في تسليط الضوء على الآثار المحتملة لاستخدام الحوسبة السحابية، كالقضايا المتعلقة بمزودي خدمات الحوسبة السحابية، والبيانات، والمدفوعات، والدعم، واستراتيجية إلغاء العقد.

8 - توثيق جميع المسائل التعاقدية ذات الصلة في اتفاقية مستوى الخدمة الشاملة (SLA) بما في ذلك متطلبات العمل الرئيسية مثل التوافر والموثوقية وقابلية التوسع واستمرارية الأعمال، والتي يجب مراجعتها والموافقة عليها من قبل مستشار قانوني.

9 - التأكد من توفير التدريب المناسب لموظفي تقنية المعلومات لضمان التعامل مع الخدمات والتطبيقات المستندة إلى السحابة وإدارتها.

13.7: يجب على المؤسسة الصحية في حال رغبتها استضافة البيانات والتطبيقات الخاصة بها خارج سلطنة عمان باستخدام الخدمات السحابية، الالتزام بالآتي:

1 - عدم وجود بدائل متاحة داخل سلطنة عمان.

2 - الحصول على موافقة مركز الدفاع الإلكتروني قبل حفظ أي بيانات صحية أو معالجتها خارج سلطنة عمان، وأن يكون الطلب مسببا.

3 - أن يكون طلب المؤسسة محددا بنطاق خدمة البرمجيات (SaaS) دون غيرها.

4 - إجراء تقييم داخلي للمخاطر لجميع البيانات الصحية والأنظمة من أجل تحديد مستوى المخاطر المرتبطة بها.

5 - الالتزام بقوانين سلطنة عمان والسياسات والمعايير والأطر الصادرة من وزارة النقل والاتصالات وتقنية المعلومات ومركز الدفاع الإلكتروني.

6 - توثيق جميع المسائل التعاقدية ذات الصلة في اتفاقية مستوى الخدمة (SLA) والتي يجب مراجعتها والموافقة عليها من قبل المستشار القانوني للمؤسسة.

7 - على مؤسسات القطاع الخاص الصحية التي تتعامل مع البيانات الحكومية الحصول على موافقة الجهات الحكومية المنظمة للنشاط كالبنك المركزي العماني وهيئة تنظيم الاتصالات.

14 تشفير البيانات:

14.1: يجب على المؤسسة الصحية تشفير البيانات والملفات قبل إرسالها فيما بينها عبر الشبكة المعلوماتية.

14.2: يجب على المؤسسات الصحية في حال نقل البيانات المشفرة فيما بينها عبر الشبكة المعلوماتية، وضع إجراء مقبول للطرفين لإدارة مفتاح التشفير عن طريق تثبيت شهادات المصادقة والتشفير على نظام البريد الإلكتروني والتأكد من استخدام بروتوكولات نقل ملفات وبرامج التشفير المعتمدة.

15 إدارة تحديث الأنظمة:

15.1: يجب على المؤسسة الصحية مواكبة التطورات التي تطرأ على وسائل تقنية المعلومات، والشبكة، ونظم المعلومات (نظم التشغيل، نظم قواعد البيانات، والنظم المرتبطة بها)، بما في ذلك إصدارات البرامج المعلوماتية والنظم المعلوماتية الجديدة، بما من شأنه حل نقاط الضعف في نظم المعلومات التي تحتوي على المعلومات الإلكترونية الصحية المحمية، وتمكين الموظفين المختصين بتقنية المعلومات من تتبع التغيير واستكشاف المشكلات التي تنشأ بسبب التحديث أو التطبيقات الجديدة أو إعادة التكوين أو أي تغيير آخر في النظام وإصلاحها.

15.2: يجب أن يكون الموظف المختص بإجراء تحديث نظم المعلومات أو تنفيذ أو تثبيت نسخ جديدة لبرامج المعلوماتي أو إعادة تشكيل تلك النظم أو تغيرها أن يكون على دراية بكيفية التراجع عن التغيير في حالة تسبب التغيير في تأثير سلبي داخل النظام وأصبح من المهم إزالته، ويتعين عليه الالتزام بالآتي:

1 - تسجيل جميع التغييرات التي قام بإجرائها على النظام المعلوماتي بدقة وعناية.

2 - التأكد مسبقا من إجراء جميع عمليات النسخ الاحتياطي للبيانات ذات الصلة قبل إجراء أي تغيير في النظام.

3 - التأكد من جودة وكفاءة عمل النسخ الاحتياطية قبل التخزين.

4 - إخطار الموظفين عن أي تغييرات أو تحديثات محورية في نظم المعلومات المستخدمة وتدريبهم عليها إذا لزم الأمر.

16 عمليات التدقيق:

16.1: يجب على المؤسسة الصحية إجراء تدقيق روتيني على أنشطة وأنظمة المستخدمين؛ من أجل التقييم المستمر للمخاطر وتحديد نقاط الخطر المحتملة على معلوماتها الصحية.

16.2: على المؤسسة الصحية في سبيل التدقيق على أنشطة وأنظمة المستخدمين، العمل على تطوير وتنفيذ وصيانة التدابير الأمنية الإدارية والمادية والفنية المناسبة وفقًا للقوانين والسياسات العامة، وعليها بصفة خاصة الالتزام بالآتي:

1 - إنشاء سجل تدقيق للتمكن من متابعة الأحداث على جميع أجهزة الحاسب الآلي والخوادم التي تقوم بمعالجة أو نقل أو تخزين البيانات الصحية.

2 - تضمين سجل التدقيق الحد الأدنى من المعلومات الأساسية، ويشمل ذلك معرف المستخدم ووقت وتاريخ تسجيل الدخول والجهاز المستخدم ونطاق بيانات المريض التي تم الوصول إليها لكل محاولة وصول.

3 - ضمان احتواء كل نظام معلوماتي على لوحة تحكم لمتابعة وتعقب أنشطة المستخدمين.

4 - تخزين مسارات التدقيق على خادم منفصل لتقليل تأثير هذا التدقيق على العمليات الأخرى.

5 - استخدام وسائل تقنية المعلومات المناسبة لكشف عمليات التسلل.

6 - إجراء تدقيق دوري على مدخلات وخرجات نظم المعلومات الصحية كالطباعة واستخدامات الإنترنت.

7 - إعداد وتوثيق قائمة بصلاحيات المستخدمين، والعمل على تحديثها باستمرار.

17 مراجعة نشاط نظم المعلومات:

17.1: يجب على المؤسسة الصحية إجراء مراجعة داخلية بشكل منتظم لنشاط نظم المعلومات لتقليل الانتهاكات الأمنية.

17.2: يجب أن تشمل مراجعة نظم المعلومات للمؤسسة الصحية كل من: حسابات المستخدمين، والدخول إلى البرامج المعلوماتية ونظم المعلومات، والوصول إلى الملفات، والحوادث الأمنية، وسجلات التدقيق، وتقارير الوصول، وذلك من خلال اتباع الضوابط الآتية:

1 - الرجوع إلى سياسة «ضوابط التدقيق» للاطلاع على الآليات التقنية التي تتبع وتسجل أنشطة نظم المعلومات التي تحتوي على المعلومات الصحية.

2 - توفير الأدوات التقنية اللازمة لإجراء المراجعة.

3 - تمتع الموظف المختص بالمراجعة بالمهارات الفنية المناسبة فيما يتعلق بنظام التشغيل والتطبيقات؛ حتى يتمكن من الوصول إلى سجلات التدقيق والمعلومات ذات الصلة وتفسيرها بشكل مناسب.

4 - تضمين تقرير نتائج المراجعة اسم الموظف المختص بالمراجعة، وتاريخ ووقت الأداء، والنتائج المهمة التي تصف الأحداث التي تتطلب اتخاذ إجراءات إضافية مثل التحقيق الإضافي أو تدريب الموظفين أو تعديلات البرنامج أو التعديلات على الضمانات.

5 - إجراء المراجعات سنويا أو عند الاشتباه في ارتكاب خطأ ما، وعند إجراء المراجعات يجب فحص سجلات التدقيق للأحداث الأمنية المهمة بما في ذلك:

أ- تتبع محاولات تسجيل الدخول غير الناجحة، وكذلك عمليات إغلاق الحساب، والوصول غير المصرح به، وتحديد عددها.

ب- تتبع المحاولات غير الناجحة للوصول إلى السجلات، وتحديد مدى تكرارها، وإنشاء سجل لعمليات الوصول غير المصرح به سواء للمراجعة أو التعديل والحذف.

ج- فحص السجلات من أجهزة الحماية أو من سجلات تدقيق النظام؛ للأحداث التي تشكل اختراقا لنظم المعلومات أو محاولات اختراق غير ناجحة أو ضارة مثل الفيروسات أو الفيروسات المتنقلة، أو رفض الخدمة، أو حوادث الفحص والتحقيق.

د- مراجعة حسابات المستخدمين في جميع نظم المعلومات؛ للتأكد من أن المستخدمين الذين لم يعد لديهم حاجة للعمل في أنظمة المعلومات لم يعد لديهم القدرة على الوصول إلى المعلومات والنظام.

6 - التزام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات باستخراج وحفظ جميع التقارير والإجراءات الموصي بها، والنظر فيها؛ لتحديد ما مدى الحاجة لإجراء تغييرات على الضمانات الإدارية والمادية والفنية للمؤسسة الصحية من عدمه.

7 - التزام التقسيم الإداري المختص بتقنية المعلومات بالفحص الأمني الشامل لوسائل تقنية المعلومات، ونظم المعلومات، والتطبيقات، والشبكات، والمواقع مرتين سنويا؛ للتأكد من سلامتها وخلوها من أي أعطال قد تهدد خصوصية وأمن المعلومات.

17.3: إذا أسفرت عملية المراجعة عن اكتشاف حادث أمني، فيجب معالجة هذا الأمر وفقا لأحكام البند ٦.٦ من هذه السياسة.

18 سلامة البيانات:

18.1: يجب على المؤسسة الصحية تطبيق الآليات الإلكترونية المناسبة للتأكد من أن المعلومات الصحية لن يتم تغييرها أو إتلافها بطريقة غير مصرح بها، وذلك من خلال اتباع الضوابط الآتية:

1 - استخدام تطبيقات ذات الذكاء المدمج (قدر الإمكان) للتحقق تلقائيًا من الأخطاء البشرية.

2 - استخدام أنظمة كشف التسلل المناسبة.

3 - توفير الأدوات التقنية المناسبة لرصد جميع التغيرات على البيانات والمعلومات الصحية بما في ذلك الحذف والإلغاء والتغيير والتحويل.

4 - استخدام نظام التشفير لتجنب أخطاء الإرسال، في أثناء إرسال البيانات بين أجهزة الحاسب الآلي

5 - الالتزام بتشفير البيانات الحساسة في قواعد البيانات حسب درجة تصنيفها ووفقا للمادة (3.8) من هذه السياسة.

6 - التحقق من عدم تكرار البيانات في أنظمة الحاسب الآلي؛ لضمان التكامل بينها.

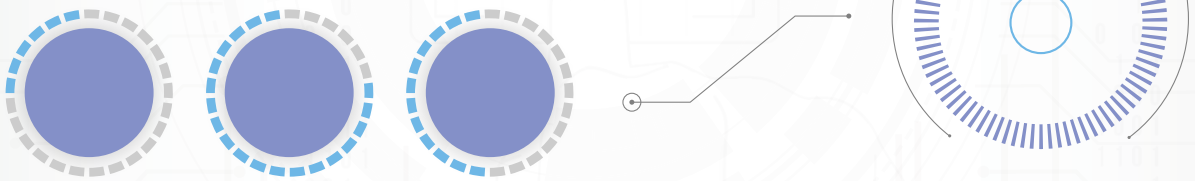
7 - اختبار أنظمة المعلومات للتأكد من أداء وظائفها ودقتها قبل البدء في استخدامها تفاديا لأخطاء البرمجة.

8 - تحديث أنظمة المعلومات عند إصدار تحديث جديد لإصلاح ومعالجة الأخطاء أو المشكلات المعروفة.

9 - تثبيت برامج مكافحة الفيروسات وتحديثها بانتظام على جميع أجهزة الحاسب الآلي لاكتشاف البرمجيات الضارة ومنعها من تغيير البيانات أو إتلافها.

10 - المحافظة على الوسائط الخارجية من التلف والتدمير والسرقة.

11 - إبقاء الوسائط الخارجية بعيدة عن المجالات المغناطيسية القوية والحرارة.



الفصـــــــل السابع

19. خطة الطوارئ

20. عملية إدارة المخاطر

21. إدارة البيانات الصحية في حالة توقف النظام عن العمل

22. الوصول للمعلومات في حالات الطوارئ (كسر الزجاج)

23. الإخطار بالاختراق

24. انتهاك الخصوصية وأمن المعلومات

25. أمن مرافق المؤسسة الصحية

19 خطة الطوارئ:

19.1: يكون التقسيم الإداري المختص بإدارة المعلومات الصحية، بعد التنسيق مع التقسيمات التنظيمية المختصة بكل من: تقنية المعلومات، والأزمات والطوارئ، مسؤولاً عن تطوير وتحديث وثيقة خطة إدارة حالات الطوارئ والتعافي من الكوارث وتحديثها؛ لضمان الآتي:

1 - استرجاع المعلومات الصحية المفقودة لأي سبب بما فيها الكوارث أو التخريب أو فشل النظام، وجعلها متاحة في الوقت المناسب.

2 - الاحتفاظ بنسخ من خطة إدارة حالات الطوارئ داخل وخارج المؤسسة الصحية.

19.2: يجب أن تتضمن خطة إدارة حالات الطوارئ والتعافي من الكوارث الآتي:

1 - النسخة الحالية من أنظمة المعلومات وتكوين الشبكات التي تم تطويرها وتحديثها كجزء من تحليل المخاطر.

2 - النسخة الحالية من إجراءات النسخ الاحتياطي المكتوبة التي تم تطويرها وتحديثها وفقًا لهذه السياسة.

3 - النماذج الورقية والوثائق اللازمة لتسجيل المريض والتوثيق الطبي والمالي.

19.3: يجب على التقسيم الإداري المختص بإدارة المعلومات الصحية تحديد فريق استجابة للطوارئ ويكون هذا الفريق مسؤولا عن الآتي:

1 - تحديد تأثير الكارثة على سير الأعمال في المؤسسة بما فيها عدم توفر نظم المعلومات الصحية.

2 - تأمين الموقع وتوفير الأمن المادي المستمر.

3 - استرجاع المعلومات الصحية المفقودة.

4 - وضع الحلول البديلة المناسبة في حال كانت أنظمة المعلومات الصحية غير متوفرة.

5 - اتخاذ الخطوات التقنية اللازمة لاستعادة سير العمل.

6 - الاحتفاظ بأرقام هواتف وعناوين البريد الإلكتروني لجميع الأشخاص الذين سيتم الاتصال بهم في حالة وقوع كارثة.

19.4: يجب أن يجتمع فريق الاستجابة للطوارئ سنويا لغرض الآتي:

1 - مراجعة مدى فعالية خطة الاستجابة للطوارئ التي قد تتعرض لها المؤسسة الصحية.

2 - عمل التدريبات اللازمة لاختبار فعالية الخطة وتقييم نتائج هذه التدريبات.

3 - مراجعة خطة الاستجابة لحالات الطوارئ والتعافي والقيام بإجراء التغييرات المناسبة عليها.

20 عملية إدارة المخاطر:

20.1: يجب على المؤسسة الصحية أن تجري تقييماً دقيقاً وشاملاً للمخاطر ونقاط الضعف المحتملة فيما يتعلق بخصوصية وأمن وتوافر المعلومات، وذلك على النحو الآتي:

1 - يكون التقسيم الإداري المختص بإدارة المعلومات الصحية والتقسيم الإداري المختص بتقنية المعلومات مسؤولين عن تنسيق وتحليل المخاطر بالمؤسسة الصحية وتحديد الأشخاص المناسبين فيها للمساعدة في تحليل المخاطر.

2 - يجب أن يتألف فريق إدارة المخاطر من أفراد ومجموعات مختلفة من المؤسسة ويجب عليهم العمل معا كفريق واحد وتحديد الأصول وتشكيل قائمة بأصول المعلومات.

3 - تحديد وتوثيق جميع أصول معلومات المؤسسة بما فيها أصول المعلومات والبيانات، والأصول التقنية، والأشخاص، والخدمة.

4 - مراعاة الآتي عند إدارة الخصوصية والأمن:

أ- تحديث وتطوير نظم المعلومات.

ب- إدراج المعلومات التالية لجميع الأجهزة (أجهزة الشبكة، الطابعات، والماسحات الضوئية، والأجهزة المحمولة) والبرامج (مثل نظام التشغيل، والتطبيقات المختلفة (تاريخ الحصول عليها، الموقع، المورد، التراخيص، جدول الصيانة.

ج- تحديث وتطوير المخطط الذي يوضح موقع جميع معدات أنظمة المعلومات، ومصادر الطاقة، ومقابس الهاتف، ومعدات الاتصالات الأخرى، ونقاط الوصول إلى الشبكة، ومعدات إنذار الحريق والسطو، وتخزين المواد الخطرة.

د- تحديد الأشخاص المخول لهم استخدام الأنظمة حسب المسمى الوظيفي ووصف الطريقة التي يتم بها منح التفويض.

هـ - بالنسبة لكل تطبيق يجب الآتي:

- وصف البيانات المرتبطة بهذا التطبيق.

- تحديد ما إذا تم إنشاء البيانات من قبل المؤسسة أو تلقيها من طرف ثالث. إذا تم استلام البيانات من طرف ثالث، حدد هذا الطرف والغرض وطريقة الاستلام.

- تحديد ما إذا كان يتم الاحتفاظ بالبيانات داخل المؤسسة فقط أو نقلها إلى أطراف ثالثة. إذا تم إرسال البيانات إلى طرف ثالث، حدد هذا الطرف والغرض وطريقة الإرسال

- تحديد مدى أهمية التطبيق والبيانات ذات الصلة على أنها عالية أو متوسطة أو منخفضة. من حيث درجة التأثير على المؤسسة إذا كان التطبيق و/ أو البيانات ذات الصلة غير متوفرة لفترة من الزمن (بالرجوع إلى إطار إدارة مخاطر تقنية المعلومات).

- تحديد حساسية البيانات بأنها عالية أو متوسطة أو منخفضة. حيث إن الحساسية هي طبيعة البيانات والضرر الذي قد ينجم عن خرق السرية أو حادث أمني (بالرجوع إلى إطار إدارة مخاطر تقنية المعلومات).

- لكل تطبيق يجب تحديد الضوابط الأمنية المختلفة المعمول بها حاليا وسياسات وإجراءات مكتوبة تتعلق بهذه الضوابط.

5 - تحديد وتوثيق التهديدات التي تتعرض لها خصوصية وأمن البيانات التي تم إنشاؤها أو تلقيها أو صيانتها أو إرسالها عن طريق المؤسسة. تشمل هذه التهديدات:

أ- التهديدات الطبيعية، مثل الزلازل وأضرار العواصف.

ب- التهديدات البيئية، مثل أضرار الحريق والدخان وانقطاع التيار الكهربائي ومشاكل المرافق.

ج- التهديدات البشرية بما فيها:

- الأعمال العرضية، مثل أخطاء الإدخال أو برمجة التطبيقات أو إجراءات المعالجة الخاطئة، أو الفشل في تحديث / ترقية البرامج / الأجهزة الأمنية، ونقص الموارد المالية والبشرية الكافية لدعم الضوابط الأمنية اللازمة.

- الأنشطة غير الملائمة، مثل السلوك غير اللائق، وإساءة استخدام الامتيازات أو الحقوق وإهدار موارد المؤسسة.

- العمليات غير القانونية والهجمات المتعمدة، مثل التنصت والتطفل والاحتيال والسرقة والتخريب والابتزاز.

6 - تحديد وتوثيق نقاط الضعف في نظم المعلومات بالمؤسسة، حيث من المهم إجراء تحليل ذاتي باستخدام المعايير ومواصفات التنفيذ لتحديد نقاط الضعف.

7 - تحديد وتوثيق احتمالية وأهمية المخاطر المحددة.

8 - تحديد مستوى الاحتمال، أي احتمال وقوع حادث أمني ينطوي على مخاطر محددة:

أ- تُعرَّف عبارة «مرجح جدًا» على أنها تنطوي على فرصة محتملة لحدوثها.

ب- يتم تعريف «المحتمل» على أنها فرصة كبيرة لحدوثها.

ج- يتم تعريف «ليس من المحتمل» على أنه فرصة متواضعة أو غير مهمة لحدوثها.

9 - تحديد مستوى تأثير الحادث الأمني:

أ- يُعرَّف «مرتفع» بأنه له تأثير كارثي على المؤسسة الصحية بما في ذلك كمية كبيرة من المعلومات الصحية التي ربما تكون قد فُقدت أو تعرضت للخطر.

ب- يتم تعريف «متوسط» على أنه له تأثير كبير بما في ذلك كمية معتدلة من المعلومات الصحية التي ربما تكون قد فُقدت أو تعرضت للخطر.

ج- يُعرَّف «منخفض» بأنه تأثير متواضع بما في ذلك فقدان بعض المعلومات الصحية غير المهمة أو تعرضها للخطر.

10 - تحديد وتوثيق التدابير والضمانات الأمنية المناسبة لمعالجة نقاط الضعف الرئيسية، حيث يجب مراجعة نقاط الضعف مع التركيز على الثغرات الأمنية عالية الخطورة.

11 - تطوير وتوثيق استراتيجية تنفيذ للتدابير والضمانات الأمنية الهامة.

12 - تقييم فعالية التدابير والضمانات بعد التنفيذ وإجراء التعديلات المناسبة.

13 - يكون قسم إدارة المعلومات الصحية مسؤولاً عن تحديد الأوقات المناسبة لإجراء تقييمات المتابعة وتنسيق هذه التقييمات. يجب على قسم إدارة المعلومات الصحية تحديد الأشخاص المناسبين داخل المؤسسة للمساعدة في مثل هذه التقييمات. يجب أن تشمل تقييمات المتابعة ما يلي:

عمليات التفتيش والمراجعة من خلال تقييم مدى كفاية الضمانات الإدارية والمادية ويجب أن يشمل هذا التقييم مقابلات لتقييم امتثال الموظف؛ عمليات التفتيش بعد ساعات العمل لتقييم الأمن المادي، وحماية كلمة المرور، مراجعة أحدث السياسات والإجراءات الأمنية للتأكد من صحتها واكتمالها؛ والتفتيش وتحليل سجلات التدريب والحوادث وتقديم توصيات للتحسين.

21 إدارة البيانات الصحية في حالة توقف النظام عن العمل

21.1: يجب على المؤسسة الصحية، وضع خطة لإدارة بيانات المريض في حالة عدم التمكن من الوصول إلى نظام السجلات الصحية الإلكترونية بسبب التوقف المخطط له أو غير المخطط له.

21.2: يجب على التقسيم الإداري المختص بتقنية المعلومات إخطار التقسيم الإداري المختص بإدارة المعلومات الصحية في أقرب وقت ممكن في الحالات الآتية:

1 - التوقف المخطط له لأنظمة السجلات الصحية الإلكترونية.

2 - الانقطاع غير المتوقع في أنظمة السجلات الصحية الإلكترونية.

3 - استئناف خدمات السجلات الصحية الإلكترونية بعد انقطاع بحيث يمكن استئناف العمليات العادية.

21.3: يجب توثيق زيارة المريض في حالة توقف نظام السجلات الصحية الإلكترونية، ويتولى مسؤولية ذلك التقسيم الإداري المختص بإدارة المعلومات الصحية، وعليه في سبيل تحقيق ذلك الآتي:

1 - إعداد أرقام تعريفية مؤقتة للمريض (بشكل مسبق) تحل محل الرقم التعريفي بنظام السجلات الصحية الإلكتروني في حال توقفه عن العمل.

2 - حظر استخدام الأرقام التعريفية المؤقتة للحالات الطارئة فقط.

3 - إعداد سجل ورقي مؤقت للمريض يدون فيه رقمه التعريفي الورقي المؤقت.

4 - تعبئة استمارات التسجيل الورقية للبيانات الديموغرافية بواسطة موظف التسجيل وإيداعها في سجل المريض الورقي.

5 - متابعة الطاقم الطبي للتحقق من التزامه بنقل البيانات من السجل الورقي إلى نظام السجلات الصحية الإلكتروني عند استعادة خدمات النظام.

6 - تخزين بيانات المريض في سجله الإلكتروني المنشأ مسبقا في حالة وجوده.

7 - تخزين بيانات المريض في سجل إلكتروني جديد يتم إنشاؤه في حالة عدم وجود سجل إلكتروني مسبق له.

22 الوصول للمعلومات في حالات الطوارئ (كسر الزجاج)

22.1: يجب على المؤسسة الصحية وضع إجراءات واضحة للوصول إلى معلومات المريض في حالات الطوارئ (كسر الزجاج) بحيث يمكن من خلالها للطاقم الطبي المصرح له الحصول على الحد الأدنى من المعلومات الصحية الضرورية لعلاجه بفعالية وكفاءة، ويجب أن يراعى فيها الضوابط الآتية:

1 - تحديد وتعريف أسباب طلب الطاقم الطبي المصرح له الوصول إلى المعلومات والبيانات الصحية للمريض في حالات الطوارئ الطبية (كسر الزجاج).

2 - رصد وتوثيق حالات وصول الطاقم الطبي المصرح له إلى المعلومات والبيانات الصحية للمريض في حالات الطوارئ الطبية (كسر الزجاج).

3 - تصنيف عمليات (كسر الزجاج) في حالات الطوارئ حسب مستوى تصنيف البيانات المدرج في البند 8.3 من هذه السياسة.

4 - وضع ميزات أمنية إضافية في حالة الحاجة إلى (كسر الزجاج) للوصول إلى بيانات عالية الحساسية في البند 8.3.1 أو المحجوبة في البند 8.13 من هذه السياسة.

5 - توفير تدريب وتوعية للطاقم الطبي المصرح له بشأن إجراءات الوصول إلى المعلومات والبيانات الصحية للمريض في حالات الطوارئ الطبية (كسر الزجاج).

22.2: تكون آلية الوصول إلى المعلومات الصحية في حالات الطوارئ (كسر الزجاج) على النحو الآتي:

1 - تقديم طلب تلقائي للنظام المعلوماتي من قبل المستخدم المصرح له بالوصول إلى تلك البيانات يبين فيه سبب طلبه.

2 - أن يتضمن سجل تتبع الوصول إلى المعلومات، البيانات الآتية كحد أدنى:

أ- اسم المستخدم المصرح له بالوصول إلى المعلومات المذكورة.

ب- مسماه الوظيفي.

ج- سبب الوصول.

د- تاريخ ووقت التصريح له بالوصول.

هـ - أي إضافة أو تعديل أو حذف يجريها.

3 - تتبع الوصول في حالات الطوارئ وتوثيقه بناء على قدرات النظم المعلوماتية، ويتولى التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات القيام بعملتي التعقب والتوثيق؛ لتحديد ما إذا كان الوصول في حالات الطوارئ كان صحيحا من عدمه.

4 - الاحتفاظ بالسجل المتعلق بتتبع الوصول في حالات الطوارئ والاحتفاظ به لمدة خمس سنوات على الأقل من تاريخ الإنشاء.

23 الإخطار بالاختراق:

23.1: يجب على الموظف أو شركاء العمل إبلاغ التقسيم الإداري المختص بإدارة المعلومات الصحية عن أي اختراق محتمل يؤثر على خصوصية وأمن المعلومات، وذلك خلال مدة لا تزيد على 24 ساعة، مع تزويده بأكبر قدر ممكن من التفاصيل.

23.2: يكون التقسيم الإداري المختص بإدارة المعلومات الصحية والتقسيم الإداري المختص بتقنية المعلومات مسؤولين عن متابعة بلاغات الاختراق واتخاذ الإجراءات اللازمة، كل في مجال اختصاصه.

23.3: يجب التقسيم الإداري المختص بإدارة المعلومات الصحية إبلاغ الإدارة العليا بالمؤسسة الصحية بحوادث الاختراق فور علمه بها.

23.4: يجب على الإدارة العليا بالمؤسسة الصحية إبلاغ وزارة النقل والاتصالات وتقنية المعلومات بحوادث الاختراق، فور علمها بها.

23.5: يجب على الإدارة العليا في المؤسسة الصحية إبلاغ مركز الدفاع الإلكتروني بحوادث الاختراق فور علمها بها، ويجب أن يتضمن البلاغ البيانات الكافية، وبصفة خاصة الآتي:

1 - تفاصيل وطبيعة البيانات المخترقة.

2 - اسم ورقم هاتف الموظف المسؤول عن متابعة الحادثة في المؤسسة الصحية.

3 - التبعات المتوقعة لحادثة الاختراق.

4 - التدابير المتخذة أو المقترح اتخاذها للتعامل مع حادثة الاختراق.

23.6: يجب على التقسيم الإداري المختص بإدارة المعلومات الصحية والتقسيم الإداري المختص بتقنية المعلومات في المؤسسة الصحية، كل في مجال اختصاصه، اتخاذ الضوابط اللازمة لاحتواء الاختراق، وذلك من خلال الآتي:

1 - وقف الممارسات غير المصرح بها.

2 - استعادة البيانات متى كان ذلك ممكنا.

3 - إغلاق النظام المعلوماتي الذي تم اختراقه.

4 - العمل على التخفيف من آثار الاختراق.

5 - وضع خطة لمعالجة نقاط الضعف في ممارسات الخصوصية والأمن والعمل على تنفيذها.

23.7: يجب على التقسيم الإداري المختص بإدارة المعلومات الصحية والتقسيم الإداري المختص بتقنية المعلومات في المؤسسة الصحية، كل في مجال اختصاصه، تقييم المخاطر من خلال اتباع الضوابط والإجراءات الوقائية اللازمة، وذلك على النحو الآتي:

1 - التحقيق في ظروف الاختراق وتحديد الأسباب الجذرية، ووضع خطة تصحيحية والعمل على تنفيذها.

2 - تقدير مدى الحاجة إلى إبلاغ الأفراد المتضررين من الاختراق بنتيجة التحقيق وتقييم المخاطر.

3 - إذا تطلب الأمر إبلاغ الأفراد المتضررين من واقعة الاختراق، يكون ذلك خلال 10 أيام عمل من تاريخ انتهاء التحقيق وتقييم المخاطر.

4 - توفير الضمانات التقنية الكافية للحد من الاختراقات مستقبلا.

5 - مراجعة الإجراءات وتحديثها على نحو يعكس الدروس المستفادة من التحقيق وتقييم المخاطر

24 انتهاك الخصوصية وأمن المعلومات:

24.1: يجب على المؤسسة الصحية في حالة وقوع حادث انتهاك خصوصية وأمن المعلومات، اتخاذ الضوابط الآتية:

1 - توثيق تفاصيل واقعة الانتهاك ويشمل ذلك:

أ- مكان ووقت وقوع الانتهاك.

ب- اسم مقدم بلاغ الانتهاك.

ج- اسم مرتكب واقعة الانتهاك.

د- اسم الشخص أو الجهة التي تم نقل البيانات إليه.

هـ- الأسباب المحتملة للانتهاك.

و- الخطوات المتخذة عند الإبلاغ بالانتهاك.

2 - إبلاغ التقسيم الإداري المختص بإدارة المعلومات الصحية بالمؤسسة الصحية عن واقعة انتهاك البيانات.

3 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع قسم تقنية المعلومات بإغلاق حساب المنتهك لحين الانتهاء من التحقيق في واقعة الانتهاك.

4 - قيام التقسيم الإداري المختص بإدارة المعلومات الصحية بالتحقيق في واقعة الانتهاك بالتنسيق مع التقسيمات الإدارية ذات العلاقة بالواقعة ووضع الحلول المناسبة لتفادي الانتهاك مستقبلا.

5 - إبلاغ التقسيم الإداري المسؤول عن خصوصية وأمن المعلومات في وزارة الصحة بتفاصيل واقعة الانتهاك.

6 - قيام التقسيم الإداري المختص في وزارة الصحة عن خصوصية وأمن المعلومات بدراسة وقائع الانتهاك بالتنسيق مع الجهات ذات العلاقة وإبلاغ المؤسسة الصحية بالتوصيات المناسبة.

25 أمن مرافق المؤسسة الصحية:

25.1: يجب على المؤسسة الصحية تعزيز حماية أصول نظم المعلومات الصحية فيها، وضمان الوصول إلى مرافقها بطريقة آمنة من خلال وضع الضوابط التالية:

1 - التزام الموظفين بارتداء بطاقات التعريف الخاصة بهم، ويحظر تمامًا إعطاء بطاقة أي موظف لشخص آخر، ويجب على موظفي الأمن ورئيس القسم المعني بالموظف التأكد من أن جميع الموظفين يرتدون البطاقات الصحيحة يومياً.

2 - ينبغي إبلاغ موظفي الأمن بخصوص أي شخص غير مصرح له يتواجد في مكان معين.

3 - يجب التأكد من أن جميع الزوار (خارج وقت الزيارة) يقومون بتسجيل الدخول في مكتب الأمن، وارتداء شارة زائر.

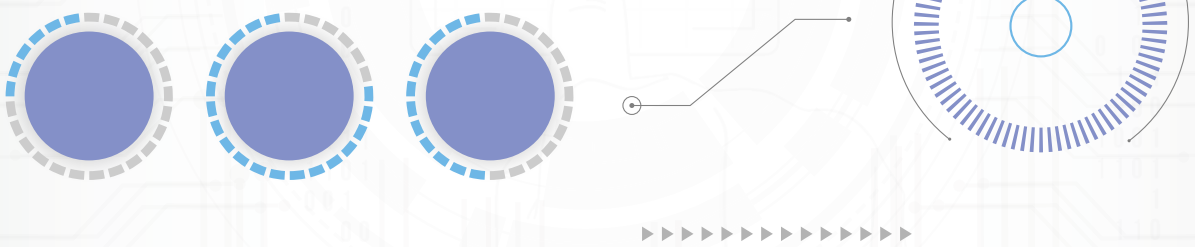
4 - يجب أن تمنح صلاحيات الدخول للموظفين حسب حاجتهم لدخول تلك الأماكن، لضمان دخول المصرح لهم فقط.

5 - يجب توفير بيئة آمنة وموثوقة للغرفة المركزية للبيانات.

6 - يجب تزويد المباني بكاميرات مراقبة لتسجيل كافة الأنشطة في المؤسسة الصحية، على وجه الخصوص الأماكن المسموح بدخولها للأشخاص المصرح لهم فقط.

7 - يجب أن يتم توفير أجهزة إطفاء الحرائق في كافة مرافق المؤسسة الصحية.

8 - يجب توفير التدريب اللازم للموظفين بكيفية اتباع إرشادات الأمن والسلامة.



الفصـــــــل الثامن

التوعية والتدريب

26 التوعية والتدريب:

26.1: يجب على المؤسسة الصحية إنشاء برامج توعوية وتدريبة مناسبة لجميع الموظفين لترسيخ مبادئ خصوصية وأمن المعلومات الصحية.

26.2: يكون حضور التدريب إلزاميًا لجميع الموظفين، ويجب على التقسيم الإداري المختص بإدارة المعلومات الصحية في المؤسسة توثيق أنشطة التدريب.

26.3: يكون التدريب لجميع الموظفين الجدد إلزاميا كجزء من عملية التعريف والتوجيه.

26.4: يتولى التقسيم الإداري المختص بإدارة المعلومات الصحية في المؤسسة مسؤولية تدريب الموظفين بالتنسيق مع الجهات ذات العلاقة ويعمل على الآتي:

1 - تطوير التدريب على الإجراءات المتبعة للحفاظ على خصوصية وأمن المعلومات الصحية.

2 - تطوير التدريب الأمني المستمر المقدم للموظفين استجابة للتغيرات البيئية والتشغيلية التي تؤثر على خصوصية وأمن المعلومات الصحية.

3 - عمل زيارات دورية ومفاجئة للأقسام والدوائر المختلفة لضمان الالتزام بالتعليمات.

26.5: يتولى التقسم الإداري المختص بإدارة المعلومات الصحية - التنسيق مع التقسيم الإداري المختص بتقنية المعلومات - مسؤولية تدريب الموظفين على كل ما يتعلق بإدارة كلمات المرور، ويشمل ذلك بصفة أساسية الآتي:

1 - التعريف بكلمة المرور.

2 - طرق التعرف على قوة كلمات المرور.

3 - طرق التعرف على كلمات المرور إذا كانت مخترقة أم لا.

4 - طرح أمثلة على سهولة كسر كلمات المرور.

5 - مشاركة الأضرار الناتجة من اختراق ومشاركة كلمات المرور.

6 - كيفية المحافظة على كلمة المرور من الكشف.

7 - كيفية تغيير كلمات المرور.

8 - الإجراءات المتبعة في حالة الاشتباه بأنه تم الكشف عن كلمة المرور.

9 - كيفية التعامل مع عروض البرامج ومواقع الإنترنت لتسجيل الدخول التلقائي.

26.6: يتولى التقسم الإداري المختص بإدارة المعلومات الصحية بالتنسيق مع التقسيم الإداري المختص بتقنية المعلومات مسؤولية تدريب الموظفين على كل ما يتعلق بمنع البرامج الضارة واكتشافها واحتوائها والقضاء عليها. ويشمل ذلك بصفة أساسية الآتي:

1 - التعريف بالإرشادات الخاصة بفتح مرفقات البريد الإلكتروني المشبوهة، والبريد الإلكتروني من مرسلين غير مألوفين، والبريد الإلكتروني الخادع.

2 - التعريف بأهمية تحديث برنامج مكافحة الفيروسات وكيفية فحص محطة عمل أو جهاز آخر لتحديد ما إذا كانت الحماية من الفيروسات حديثة أم لا.

3 - التعريف بتعليمات عدم تنزيل الملفات مطلقًا من مصادر غير معروفة أو مشبوهة.

4 - التعريف بعلامات وشواهد وجود فيروس محتمل يمكن أن يتسلل عبر برنامج مكافحة الفيروسات أو قد يصل قبل تحديث برنامج مكافحة الفيروسات.

5 - التعريف بأهمية النسخ الاحتياطي للبيانات الهامة بشكل منتظم وتخزين البيانات في مكان آمن.

6 - التعريف بالأضرار التي تسببها الفيروسات.

7 - التعريف بالإجراءات التي يجب اتباعها عند اكتشاف فيروس.

26.7: يجب على التقسيم الإداري المختص بإدارة المعلومات الصحية - بالتنسيق مع قسم تقنية المعلومات - وضع تعليمات دورية ومستديمة بشأن سياسات الخصوصية، والأمن، وأمان كلمات المرور، والبرامج الضارة، وتحديد الحوادث والاستجابة لها، والتحكم في الوصول، وضمان وصولها إلى جميع الموظفين بكافه الطرق، ومن ذلك، البرامج التوعوية والتدريبية، ورسائل البريد الإلكتروني، وشاشات التوقف، ولافتات تسجيل الدخول وغيرها، ويجب أن يكون الوصول لسياسة الخصوصية والأمن متاحاً بسهولة لجميع الموظفين.