١٠٤

قانون "قابلية نقل ومسئولية التأمين الصحي" وما يعنيه للهندسة الإكلينيكية

Health Insurance Portability and Accountability Act (HIPAA) and Its Implications for Clinical Engineering

Stephen L. Grimes
Senior Consultant and Analyst, GENTECH, Saratoga Springs, NY

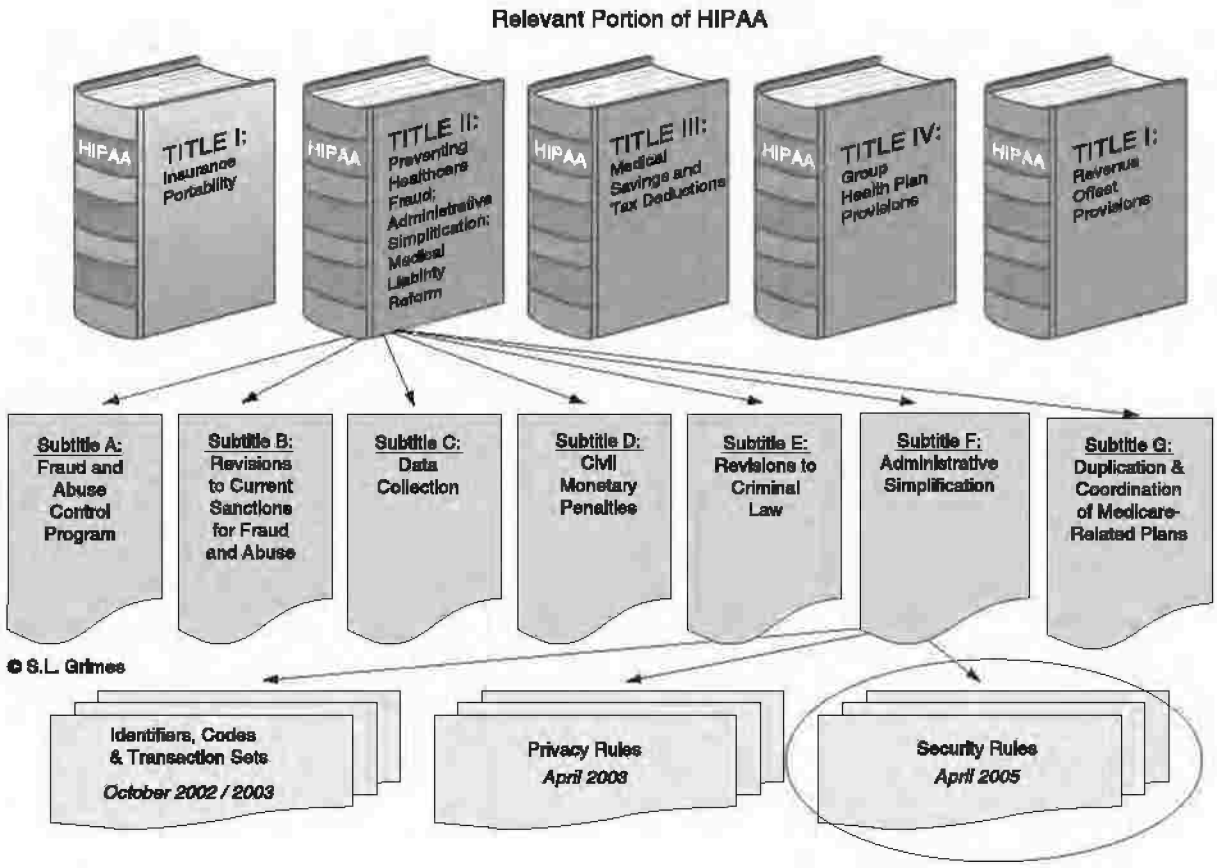
لماذا يوجد هذا الفصل عن قانون قابلية نقل ومسئولية التأمين الصحي (HIPAA) في كتاب المرجع في الهندسة الإكلينيكية؟ يمكن تفهم مثل هذا السؤال! بالحكم فقط من خلال الاسم فإن معظم القراء سوف يتوقعون أن يجدوا مناقشة بشأن التأمين الصحي والتمويل، وهو أمرٌ يمكن تفهمه أيضاً. ولكن من خلال التأمل في هذا القانون فإن القارئ يعثر على أهم جزء من تشريع الرعاية الصحية منذ تم توقيع "الرعاية الطبية" (Mdicare) ليُصبح قانوناً في عام ١٩٦٥. ومن خلال إمعان النظر في متاهة هذا التشريع والقوانين المرتبطة به فإننا نجد أن HIPAA يُدخل معايير تتطلب تغييرات واسعة في عمليات الرعاية الصحية فضلاً عن الطريقة التي يتم بموجبها اعتماد وتنفيذ التكنولوجيا.

أصول قانون "قابلية نقل ومسئولية التأمين الصحي"

The Origins of HIPAA

تم توقيع HIPAA (والمعروف أيضاً باسم القانون العام ١٠٤- ١٩١ أو مشروع قانون Kassebaum-Kennedy) ليُصبح قانوناً من قِبَل الرئيس كلينتون في عام ١٩٩٦ (لمزيد من المعلومات حول القانون العام ١٠٤-١٩١ انظر http://www.cms.hhs.gov/hipaa hipaa2/general/background/pl104191.asp). نشأ القانون الأصلي خلال إدارة بوش الأولى وتم إدراجه في وقتٍ لاحق في مبادرة إصلاح الرعاية الصحية لإدارة الرئيس بيل كلينتون. كما يوحي الاسم، فقد كان المقصود أصلاً من HIPAA أن يوفر وسيلة للمستهلكين للحفاظ على تغطية التأمين الصحي بغض النظر عن حالة توظيفهم. كما يحدث مع معظم التشريعات من نقطة كونها مفهوماً إلى نقطة تمريرها، فقد أضيفت

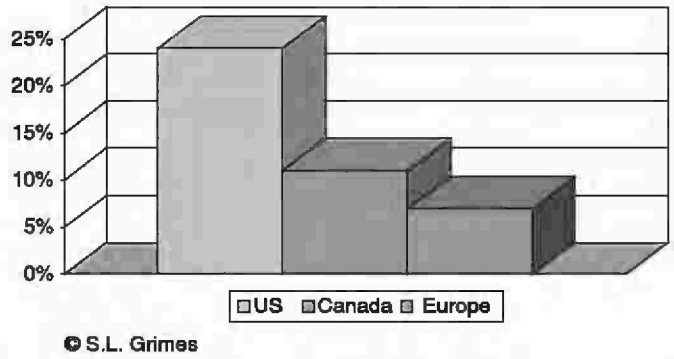
أحكام هامشية على مشروع القانون هذا. يُعتبر الحكم الذي سُمي "حكم التبسيط الإداري" من أهم هذه الأحكام (الشكل رقم ١٠٤,١).



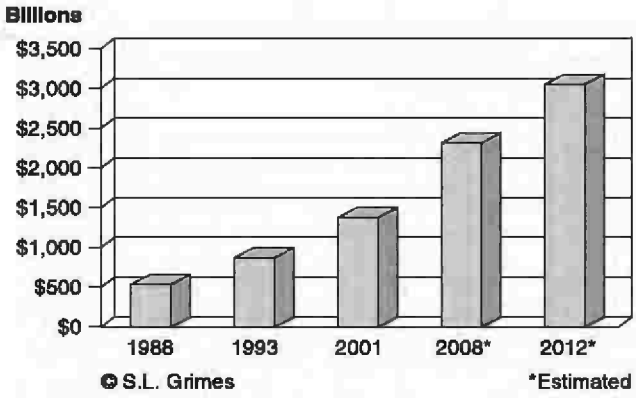
الشكل رقم (١٠٤,١). يُمثل التبسيط الإداري (العنوان الفرعي F) جزء صغير من قانون HIPAA ولكنه مسئول عن جزء كبير من تأثير HIPAA على صناعة الرعاية الصحية.

تم إضافة "التبسيط الإداري" إلى HIPAA لمعالجة مشكلة تنبَّه إليها الكونغرس في بداية تسعينيات القرن الماضي. نشرت مجلة New England Journal of Medicine في عام ١٩٩١ مقالاً يذكر أن ١٩ إلى ٢٤ سنتاً من كل دولار ينفق في الولايات المتحدة على الرعاية الصحية يتجه نحو التكاليف "الإدارية" (Woolhandler و Himmelstein، ١٩٩١) مقارنةً مع ١١٪ في كندا و٧٪ في معظم بلدان أوروبا (الشكل رقم ١٠٤,٢ أ). يرجع السبب الكبير لهذه التكاليف الإدارية إلى عدم كفاءة الصناعة حيث كانت ٧٠٪ من البيانات المُدخلة يدوياً إلى كمبيوترات الصناعة ناتجة من أجهزة كمبيوتر الأخرى، وفي الوقت نفسه كانت الصناعة متورطة بالإعداد اليدوي للملفات وعمليات النسخ

والتعامل بالفاكس والاتصالات الهاتفية والبريد (Moynihan، ٢٠٠٣). يمكن للمشكلة أن تزداد سوءاً. ففي عام ١٩٨٨ أنفقت الولايات المتحدة ٥٥٨ مليار دولار على الرعاية الصحية أو ١١٪ من ناتجها المحلي الإجمالي "GDP" (Heffler et al، ٢٠٠٣). ارتفعت هذه النفقات بحلول عام ٢٠٠١ إلى ١,٤٢٥ مليار دولار أو ١٤.١ في المائة الـ GDP. ومن المتوقع أن ترتفع بحلول عام ٢٠١٢ إلى ٣.١ تريليون دولار أو ١٧.٧٪ من الـ GDP (الشكل رقم ١٠٤.٢ ب). تم في عام ١٩٩٤ إعلام الكونغرس بأحد الحلول الممكنة لمشكلة تصاعد تكاليف الرعاية الصحية. في ذلك العام ادعى التقرير الذي أعدته مجموعة صناعة قديرة (مجموعة العمل للتبادل الإلكتروني للبيانات "WEDI") أنه يمكن لصناعة الرعاية الصحية أن توفر ٧٣ مليار دولار سنوياً إذا ما اعتمدت على التبادل الإلكتروني للبيانات (EDI) في معظم المعاملات الإدارية والمالية كما فعلت الكثير من الصناعات الأخرى في الولايات المتحدة (Duncan et al، ٢٠٠١). أدرك الكونغرس بأن طبيعة المعاملات الإلكترونية تجعل الصناعة ضعيفة بطرق على عكس نظائرها الورقية حيث أضاف متطلبات من أجل الخصوصية والأمن إلى حكم التبسيط الإداري لقانون HIPAA.



الشكل رقم (١٠٤,٢ أ). النسبة المئوية من إجمالي نفقات الرعاية الصحية المطلوبة لتغطية التكاليف الإدارية.



الشكل (١٠٤,٢ ب). الاتجاه العام في نفقات الرعاية الصحية في الولايات المتحدة.

مع كتابة القانون كانت وزارة الصحة والخدمات البشرية (HHS) مسئولة عن صياغة اللائحة الفعلية للمعاملات ومجموعات الكودات (TCS) واللائحة الأمنية. وجَّه القانون وزارة الصحة والخدمات البشرية إلى الاستفادة من خبرات منظمات الصناعة المختلفة بما في ذلك اللجنة الوطنية للإحصاءات الحيوية والصحية (NCVHS) عند وضع هذه القوانين. أعطى الكونغرس نفسه ٣٦ شهراً ضمن HIPAA لإعداد لائحة الخصوصية مع عودة هذه المسؤولية مرة أخرى إلى HHS فقط إذا فشل الكونغرس بإكمال المهمة في إطار الوقت المخصص. وبالفعل فقد فشل الكونغرس بذلك وفي نهاية المطاف أخذت الـ HHS على عاتقها مهمة صياغة لائحة الخصوصية أيضاً.

وفقاً للقانون، أعدت الـ HHS مشروع لكل لائحة ونشرته كإشعار لإحداث لائحة مقترحة (Notice of Proposed Rule Making, "NPRM") للملاحظات في السجل الفدرالي. ثم أُعطي الجمهور فترة ٦٠ يوماً للملاحظات قامت بعدها الـ HHS بإعداد اللائحة النهائية مع أخذ تلك الملاحظات بعين الاعتبار. بعد نشر اللائحة النهائية في السجل الفدرالي أُعطيت فترة مراجعة لمدة ٦٠ يوماً تلاها فترة سماح لمدة ٢٤ شهراً قبل أن تُصبح اللائحة نافذة المفعول (باستثناء الخطط الصحية الصغيرة التي مُنحت ١٢ شهراً إضافياً للامتثال). خطّط الكونغرس لأن تكون أحكام الـ TCS والخصوصية والأمن لقانون HIPAA جاهزة بحلول عام ٢٠٠٠. إلا أن الكونغرس قدَّم تمويلاً قليلاً لـHHS لبدء العملية كما استهلكت قضية الـ Y2K بشكلٍ سريع موارد الصناعة (انظر الفصل ١٠٥). بمنع حدوث تأخيرات كبيرة أخرى، فإن آخر القوانين الرئيسية لـ HIPAA سوف تصبح سارية المفعول بحلول إبريل من عام ٢٠٠٥.

نظرة عامة على أحكام التبسيط الإداري لـ HIPAA: لائحة الـ TCS ولائحة الخصوصية واللائحة الأمنية
Overview of HIPAA's Administrative Simplification Provisions: TCS, Privacy, and Security Rules

إن اللوائح الثلاث الكبرى المرتبطة بالتبسيط الإداري هي المعاملات ومجموعات الكودات والخصوصية والأمن. أنهت الـ HHS هذه اللوائح على مدى ما يقرب من ثلاث سنوات حيث بدأت بالـ TCS في أكتوبر ٢٠٠٠ وانتهت بالأمن في أبريل ٢٠٠٣. فيما يلي لمحة موجزة عن كل لائحة من هذه اللوائح:

لائحة المعاملات ومجموعات الكودات Transaction and Code Sets (TCS) Rule

لقد كان تاريخ الامتثال للائحة المعاملات ومجموعات الكودات (TCS) في ١٦ أكتوبر ٢٠٠٣. مُدِّد التطبيق لعامٍ واحد بالنسبة إلى خطط الصحة الصغيرة (أي ذات العائدات السنوية الأقل من ٥ مليون دولار) ولتلك التي قدمت طلباً للحصول على تمديد مدته سنة واحدة (في إطار ASCA). أما الكيانات المشمولة (عدا الخطط الصحية الصغيرة) والتي لم تُقدم طلباً من أجل التمديد لسنة واحدة قبل ١٥ أكتوبر ٢٠٠٢ وجب عليها أن تلتزم اعتباراً من ١٦ أكتوبر ٢٠٠٢. أما السلطة المُنفذة فهي مراكز خدمات الرعاية الطبية (Medicare) والمساعدة الطبية (Medicaid) التابعة لـ HHS (CMS).

إن لائحة الـ TCS هي قلب التبسيط الإداري ومصدر أي وفورات متوقعة في التكاليف. تدعو اللائحة إلى اعتماد المعاملات الموحدة ومجموعات الكودات في الخطط الصحية ومراكز تبادل معلومات الرعاية الصحية ومقدمي الرعاية الصحية الذين ينقلون المعلومات الصحية في شكلٍ إلكتروني بما يتعلق بأي من المعاملات المبينة فيما يلي.

تُعرَّف المعاملات الموحَّدة بمواصفات X12N للمعهد الوطني الأمريكي للمعايير X12N (ANSI) وتُعالج ما يلي:

- دفع القسط/التحويلات.
- المطالبة بالرعاية الصحية/القاء.
- انتساب إلى خطة/ فك الانتساب.
- الأهلية للحصول على خطة صحية.
- تنسيق الفوائد.
- دفع المطالبات/المشورة بخصوص التحويلات.
- حالة المطالبة بالحصول على الرعاية الصحية.
- إحالات الترخيص والتخويل.
- مُرفق المطالبة بالحصول على الرعاية الصحية (قيد التطوير- سجلات HL7).
- التقرير الأول للإصابة.

أما مجموعات الكودات الموحَّدة فقد أُخذت من الإصدارات المُحدَّدة بما يلي:

- التصنيف الدولي للأمراض (ICD).
- المصطلحات الإجرائية الحالية لـ AMA (CPT).
- الكودات الوطنية للعقاقير لـ HHS (NDC).
- نظام ترميز الإجراءات العامة للإدارة المالية للرعاية الصحية (HCPCS).
- كودات الـ ADA المتعلقة بإجراءات وتسميات طب الأسنان.
- المجلس الوطني برامج العقاقير الطبية (NCPDP).

تُعالج هذه الكودات الموحدة ما يلي:

- التشخيصات.
- العلاجات.
- الإجراءات.

- الاختبارات.
- الخدمات.
- العقاقير.
- اللوازم والمعدات.

لائحة الخصوصية Privacy Rule

إن تاريخ الامتثال لهذه اللائحة هو ١٤ إبريل ٢٠٠٣ باستثناء الخطط الصحية الصغيرة فقد حصلت على ١٢ شهراً إضافياً كفترة سماح. أما سلطة التنفيذ فهي مكتب للحقوق المدنية لـ HHS (OCR).

تُغطي لائحة الخصوصية الخطط الصحية ومراكز تبادل معلومات الرعاية الصحية ومقدمي الرعاية الصحية الذين ينقلون أي معلومات صحية بشكلٍ اكتروني. تفرض اللائحة على هذه الكيانات المشمولة وضع وتنفيذ بعض السياسات والإجراءات على النحو التالي:

- الحد من الوصول إلى المعلومات الصحية المُحدِّدة لهوية المريض بشكلٍ فردي (IIHI) بأي شكل من الأشكال (أي الإلكتروني والمكتوب والشفوي) إلى تلك المعلومات المطلوبة من قبل أولئك الذين يحتاجونها من مبدأ مشاركتهم في العلاج ودفع الرسوم أو عمليات الرعاية الصحية (TPO) إلا إذا خَوَّل المريض بشكلٍ صريح إمكانية الوصول الأوسع لهذه المعلومات.
- إعطاء المرضى الحق في الوصول إلى ملفاتهم الطبية وطلب إجراء تصحيحات لهذه السجلات والحق في معرفة الجهات التي وصلت إلى تلك السجلات.
- إجبار شركاء العمل (الذين قد يصلوا إلى الـ IIHI نتيجةً لعملهم) على اعتماد سياسات وإجراءات الخصوصية المتفقة مع متطلبات هذه اللائحة.
- تطبيق العقوبات المناسبة على أي شخص أو شريك عمل يحصل أو يستخدم بشكل غير لائق معلومات الـ IIHI الخاصة بالمريض.

اللائحة الأمنية Security Rule

إن تاريخ الامتثال للائحة الأمنية هو ٢١ إبريل ٢٠٠٥ باستثناء الخطط الصحية الصغيرة فقد حصلت على ١٢ شهراً إضافياً كفترة سماح. أما سلطة التنفيذ فهي مراكز خدمات الرعاية الطبية (Medicare) والمساعدة الطبية (Medicaid) التابعة لـ HHS (CMS).

تُغطي اللائحة الأمنية أيضاً الخطط الصحية ومراكز تبادل معلومات الرعاية الصحية ومقدمي الرعاية الصحية الذين ينقلون المعلومات الصحية بشكلٍ إلكتروني إلى أي من المعاملات المشمولة. تنطبق اللائحة على المعلومات

الإلكترونية الصحية المحمية (ePHI) التي يتم إرسالها أو حفظها في وسائط إلكترونية، كما حذرت الـ HHS "أنه قد يتم اقتراح معايير لأمن جميع المعلومات الصحية أو المعلومات الصحية المحمية الموجودة في شكلٍ غير إلكتروني في موعدٍ لاحق".

تفرض اللائحة على الكيانات المشمولة أن تضمن سرية وسلامة وتوفر الـ ePHI عن طريق تأسيس ما يلي:

- الضمانات الإدارية:
  - عمليات إدارة الأمن التي تشمل التحليل الفعال للمخاطر وبرنامج فعال لإدارة المخاطر.
  - أمن القوى العاملة (على سبيل المثال، الترخيص والتصريح والجزاءات).
  - حادث الأمن (على سبيل المثال، استجابة وتقديم التقارير).
  - تعليم وتدريب القوى العاملة على قضايا الأمن.
  - خطط الطوارئ (على سبيل المثال، تحليل الحرجية والاحتياط والتعافي من الكوارث).
  - تقييم فعالية برنامج الأمن.
  - عقود شركاء الأعمال.
- الضمانات المادية:
  - الوصول إلى المنشأة (على سبيل المثال، الطوارئ والأمن ومراقبة الدخول والصيانة).
  - استخدام وأمن محطة العمل.
  - ضبط الأجهزة والوسائط (على سبيل المثال، كيفية التخلص منها والنسخ الاحتياطي والمساءلة).
- الضمانات التقنية:
  - ضوابط الوصول (على سبيل المثال، تحديد هوية المستخدم والتشفير والوصول في حالات الطوارئ).
  - مراجعة الضوابط (على سبيل المثال، تتبع نشاط الوصول أو الدخول).
  - النزاهة (على سبيل المثال، تأصيل أو توثيق الـ ePHI).
  - أمن النقل(ضوابط السلامة والتشفير).
- المتطلبات التنظيمية:
  - عقود شركاء الأعمال.
- مُتطلبات السياسات والإجراءات والوثائق:
  - ضرورة امتثال السياسات والإجراءات للمعايير.

- الوثائق (على سبيل المثال، الاحتفاظ بسجلات إجراءات أو أنشطة أو تقييمات الامتثال).

يحمل عدم الامتثال لأحكام التبسيط الإداري لـ HIPAA في طياته خطر عقوبات مدنية وجنائية كبيرة. هناك غرامات مدنية لتصل إلى ١٠٠ دولار لكل مخالفة ويمكن أن تصل إلى حد أقصى قدره ٢٥,٠٠٠ دولار سنوياً لانتهاكات مماثلة. باعتبار أن أي فشل في الامتثال يمكن أن ينطوي على انتهاكات لمعايير متعددة فيمكن للعقوبات الفعلية الإجمالية لكل حادث أن تتجاوز الحدود القصوى الفردية. تتراوح العقوبات الجنائية من ٥٠,٠٠٠ دولار والسجن لمدة سنة واحدة لأي شخص يحصل على المعلومات الصحية المحمية، إلى ٥٠,٠٠٠ دولار والسجن لمدة خمس سنوات لأي شخص يحصل على المعلومات الصحية المحمية تحت ذرائع زائفة، إلى ٢٥٠,٠٠٠ دولار والسجن لمدة عشرة سنوات لأي شخص يحصل على المعلومات الصحية المحمية بقصد استخدامها لأغراض المنفعة التجارية أو تحقيق مكاسب شخصية أو أذى خبيث.

تأثير قانون "قابلية نقل ومسئولية التأمين الصحي" (HIPAA) على الهندسة الإكلينيكية

HIPAA's Effect on Clinical Engineering

على مدى السنوات القليلة المقبلة، ستكون جهود الامتثال مع HIPAA أمراً ذا أولوية عالية على جدول أعمال ما يُقارب من ١,٢ مليون من مُزودي الرعاية الصحية في الولايات المتحدة. تشمل قائمة هؤلاء المُزودين على المستشفيات والمختبرات ومراكز التصوير والجراحة والعيادات والصيدليات وممارسات الأطباء وغيرها من الممارسات الإكلينيكية.

سوف تستهلك HIPAA جزءاً كبيراً من موارد المستشفى. فمن المقدر أن HIPAA سيكلف المستشفيات أكثر من ٤٣ مليار دولاراً لتنفيذه (Lageman و Melick، ٢٠٠٠) بالمقارنة مع ٨,٥ مليار دولار أُنفِقَت في المستشفيات لمعالجة مشكلة Y2K (Marietti، ١٩٩٩).

تتوافق المصالح الإستراتيجية لمنظمات تزويد الرعاية على نحو وثيق مع الامتثال لـ HIPAA. تُعتبر كل وحدة تنفيذية داخل منظمة تزويد الرعاية (بما في ذلك الهندسة الإكلينيكية) ملزمة باستخدام الموارد المناسبة والمتاحة لمساعدة المنظمة في تحقيق الامتثال. في حين تُشارك الهندسة الإكلينيكية جزء من العبء الكلي للامتثال لـ HIPAA مع الوحدات التنفيذية الأخرى، فإن أثرها الأكبر سيكون في الامتثال إلى اللائحة الأمنية.

وضعت اللائحة الأمنية لقانون HIPAA لحماية سلامة وتوافر وسرية المعلومات الصحية أو البيانات المرتبطة بالمريض. ويشمل ذلك على البيانات في السجلات الطبية وسجلات الفواتير الموجودة في أنظمة المعلومات لمزود الرعاية وكذلك البيانات التشخيصية والعلاجية الموجودة في الأجهزة الطبية الحيوية وأنظمة المعلومات الإكلينيكية. وفي الواقع تُمثل الأجهزة والأنظمة الطبية الحيوية المستخدمة من قبل مقدمي الرعاية الصحية مجال خطر كبير ومتزايد

فيما يتعلق بالقضايا الأمنية لـ HIPAA. قد تكون الكمية الإجمالية للأجهزة والأنظمة الطبية الحيوية في المستشفى النموذجي ٣٠٠٪ إلى ٤٠٠٪ أكثر من عدد من أجهزة أو أنظمة تكنولوجيا المعلومات في نفس المستشفى. يمكن أن تُشكل الأنظمة المتأثرة بقانون HIPAA والمندرجة في مخزون تكنولوجيا المعلومات والأجهزة الطبية الحيوية جزءاً كبيراً من إجمالي الأنظمة في المستشفى. هناك اتجاهان رئيسيان يساهمان في أهمية المخاطر المتعلقة بالتكنولوجيا الطبية الحيوية:

١- يجري تصميم وتشغيل الأجهزة والأنظمة الطبية الحيوية كأجهزة كمبيوتر خاصة ذات ميزات آلية إضافية. يؤدي ذلك إلى كميات متزايدة من بيانات الصحة التي يجري جمعها وتحليلها وتخزينها في هذه الأجهزة.

٢- هناك نمو سريع في تكامل وترابط الأجهزة والأنظمة الطبية الحيوية وأجهزة وأنظمة تكنولوجيا المعلومات حيث يتم تبادل المعلومات الصحية.

في حين أن التكنولوجيا الطبية الحيوية تُشكل مستودعاً كبيراً للمعلومات الصحية فإنه غالباً ما يتم التغاضي عن هذه الأجهزة والنظم في منهجية أمن قانون HIPAA التي غالباً ما ترتكز على تكنولوجيا المعلومات.

إن الأمن هو قضية تهم تكنولوجيا الطب الحيوي لأن أي خلل في سلامة الـ ePHI وتوافرها يمكن أن يؤدي إلى سوء التشخيص أو العلاج للمريض. قد يؤدي العلاج غير الملائم أو تأخر العلاج إلى الضرر أو حتى الموت. كما يمكن أن يؤدي أي خلل في السرية على المساس في خصوصية المريض وربما يتسبب في خسائر مالية للمريض و/أو للمنظمة المزودة للرعاية.

من أجل معالجة أمن الـ HIPAA بنجاح يجب أن يكون المهندسون الإكلينيكيون على استعداد لتبني عقلية مختلفة. يجب على المهندسين الإكلينيكيين اتباع إدارة التكنولوجيا من وجهة النظر الأمنية مع إدراك بأن ضمان سلامة وتوافر (فضلاً عن سرية) المعلومات الصحية هو قلب البرنامج الفعال لإدارة التكنولوجيا.

نظرة مُعمقة على اللائحة الأمنية
A Closer Look at the Security Rule

تهدف اللائحة الأمنية لـ HIPAA إلى ضمان نزاهة وتوافر وسرية جميع المعلومات الصحية الإلكترونية المحمية (ePHI) والتي يُنشئها أو يتلقاها أو يُحافظ عليها أو ينقلها مزود الرعاية. تُعرف النزاهة والتوافر والسرية لأغراض الأمن على النحو التالي:

- النزاهة: عدم تغيير أو تخريب البيانات بطريقة غير مشروعة.
- التوفر: أن تكون البيانات متاحة وقابلة للاستعمال عند الطلب من قبل مستخدم مُخوَّل.
- السرية: عدم إتاحة أو كشف البيانات لأي شخص غير مُخوَّل.

وهناك القليل من التعاريف الرئيسية الأخرى المرتبطة باللائحة الأمنية وتشمل على ما يلي :

- المعلومات الصحية الإلكترونية المحمية (ePHI) هي المعلومات الصحية المُحدِّدة لهوية الفرد (IIHI) التي يتم إرسالها أو في الحفاظ على وسائط الإلكترونية.
- المعلومات الصحية المُحدِّدة لهوية الفرد (IIHI) هي المعلومات التي تُشكل مجموعة فرعية من المعلومات الصحية وتشمل المعلومات الديموغرافية التي يتم جمعها من الفرد.

١- تم إنشاؤها من قِبَل مقدمي الرعاية الصحية أو التي تلقاها مقدمي الرعاية الصحية.

٢- تتصل بالحالة الصحية السابقة أو الحالية أو المستقبلية للفرد، وتوفير الرعاية الصحية للفرد.

- تُحدد شخصية الفرد.
- تتعلق بوجود أساس معقول للاعتقاد بأن المعلومات يمكن أن تُستخدم لتحديد هوية الفرد.

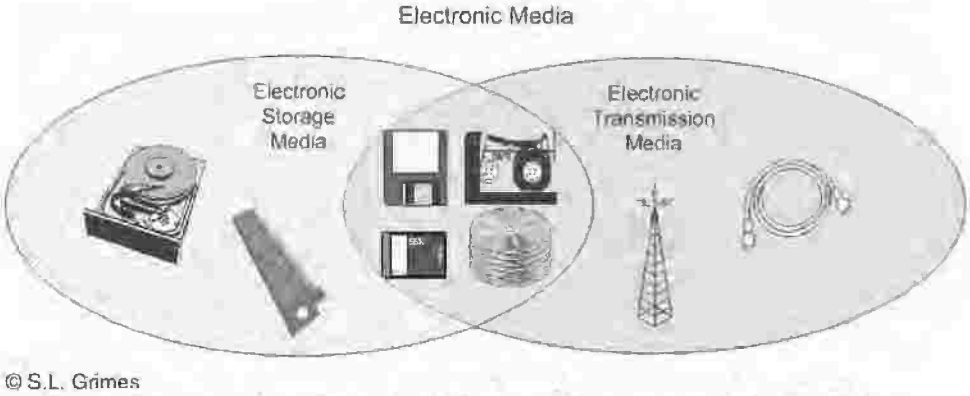
- إن الوسائط الإلكترونية (الشكل رقم ١٠٤,٣) هي :

١- وسائط التخزين وتشمل :

- أجهزة الذاكرة.
- وسائط الذاكرة الرقمية القابلة للإزالة/النقل (مثل الشريط أو القرص المغنط والأقراص الضوئية وبطاقة الذاكرة الرقمية).

٢- وسائط النقل المُستخدمة لتبادل المعلومات الموجودة بالفعل في وسائط التخزين الإلكترونية بما في ذلك :

- الإنترنت والإكسترانت (Extranet).
- خطوط الاتصال الهاتفي والخطوط المؤجرة.
- الشبكات الخاصة.
- الحركة المادية لوسائط التخزين الإلكترونية القابلة للإزالة/للنقل.



الشكل رقم (١٠٤,٣). الوسط الإلكتروني كما تم تعريفه في اللائحة الأمنية لـ HIPAA .

كُتبت اللائحة الأمنية على أن تكون مرنة. سُمح لمقدمي الرعاية باستخدام أي تدبير من التدابير الأمنية التي تمكنهم من تنفيذ المُتطلبات بشكلٍ معقول ومناسب. يجب على مقدمي الرعاية عند اختيار الإجراءات الأمنية التي سوف يستخدمونها أن يأخذوا بعين الاعتبار ما يلي:

- حجم وتعقيد وقدرات المؤسسة.
- البنية التحتية التقنية والأجهزة والبرمجيات والقدرات الأمنية للمنظمة.
- تكاليف التدابير الأمنية.
- احتمال وخطورة المخاطر المحتملة على السرية والسلامة وتوافر الـ ePHI.

تُقدم اللائحة الأمنية متطلباتها على شكل سلسلة من المعايير. إن المعايير هي مجموعة من السياسات أو الممارسات أو الخدمات أو الأنظمة المطلوبة والتي يجب على مزود الرعاية تنفيذها من أجل أن يكون في امتثال مع اللائحة الأمنية. كما تُقدم اللائحة الأمنية سلسلة من مواصفات التنفيذ المرتبطة بمعظم المعايير. إن مواصفات التنفيذ هي بمثابة المبادئ التوجيهية لسبل تلبية معيار معين. تُصنِّف اللائحة الأمنية مواصفات التنفيذ المُقدمة على أنها إما "مطلوبة (required)" أو "قابلة للمعالجة (addressable)". يجب على مزود الرعاية استخدام مواصفات التنفيذ "المطلوبة" لتلبية المعايير الخاصة بها. ينبغي على مزود الرعاية استخدام مواصفات التنفيذ "القابلة للمعالجة" لتلبية المعايير الخاصة بها ما لم يثبت مُزود الرعاية أنه يمكن أن يفي بالمعيار من خلال بديل معقول ومناسب. تشمل العوامل التي تبرر استخدام مخططات بديلة لتلبية المعايير على نتائج تحليل المخاطر وإستراتيجيات التخفيف من المخاطر ووجود أي تدابير أمنية قائمة بالفعل وتكلفة التنفيذ. عندما يتم اتخاذ خطط بديلة فيجب توثيق عملية اتخاذ القرار وأساليب التنفيذ المُختارة توثيقاً جيداً.

تنقسم معايير ومواصفات التنفيذ اللائحة الأمنية إلى الفئات التالية:

١- الضمانات الإدارية وتشمل:

تدابير رسمية موثقة (بما في ذلك السياسات والإجراءات) لإدارة عملية اختيار وتطوير وتنفيذ التدابير الأمنية لحماية البيانات الإلكترونية للقوى العاملة في ما يتعلق بحماية البيانات الإلكترونية.

٢- الضمانات المادية وتشمل:

تدابير لتوفير الحماية المادية لأنظمة تخزين أو نقل البيانات الصحية والمباني والمعدات المتصلة بها من:

- المخاطر الطبيعية والبيئية (مثل الحرائق والفيضانات).
- الاقتحام (أي استخدام الأقفال والمفاتيح والتدابير الإدارية لمراقبة الدخول).

٣- الضمانات التقنية وتشمل:

التدابير التقنية لحماية أنظمة تخزين أو نقل البيانات الصحية بالأساليب التالية :

٤- حماية /الإجراءات والتوثيق وتشمل :

- تدابير لضمان امتثال السياسات والإجراءات مع معايير ومواصفات التنفيذ للائحة الأمنية وكذلك توثيق جميع الأعمال والأنشطة الوصول إلى المعلومات.
- ضبط ومراقبة الوصول إلى المعلومات ونشاط النظام.
- التحقق من سلامة البيانات.
- ضمان التوافر.
- ضمان أمن النقل.

٥- المتطلبات التنظيمية وتشمل :

استخدام اتفاقات شريك العمل لإجبار الوكلاء والمتعاقدين الثانويين والبائعين والاستشاريين وغيرهم ممن قد يصلوا إلى المعلومات الصحية الإلكترونية المحمية على استخدام التدابير الأمنية المناسبة للحفاظ على الـ ePHI.

مُتطلبات السياساتوالتقييمات التي تُجرى بخصوص هذه المتطلبات.

يُبين الجدول رقم (١٠٤,١) مصفوفة مفصلة عن معايير ومواصفات التنفيذ للائحة الأمنية.

الجدول رقم (١٠٤,١). اللائحة الأمنية النهائية لـ HIPAA – مصفوفة المعايير ومواصفات التنفيذ.

الضمانات الإدارية		
القسم	**المعايير**	**مواصفات التنفيذ**
164.308(a)(1)	(i) عملية إدارة الأمن. تنفيذ السياسات و الإجراءات لمنع وكشف واحتواء وتصحيح المخالفات أمنية	(A) تحليل المخاطر (مطلوب). إجراء تقييم دقيق وشامل للمخاطر المحتملة ومواطن الضعف لسرية وسلامة وتوافر المعلومات الصحية الإلكترونية المحمية في حوزة الكيان المشمول (B) إدارة المخاطر (مطلوب). تنفيذ التدابير الأمنية الكافية للحد من المخاطر ومواطن الضعف إلى المستوى المعقول والمناسب من أجل الامتثال للقسم 164.306(a) (C) سياسة الجزاء (مطلوب). تطبيق العقوبات الملائمة ضد أفراد القوى العاملة الذين لا يمتثلون للسياسات والإجراءات الأمنية للكيان المشمول (D) مراجعة نشاط نظام المعلومات (مطلوب). تنفيذ إجراءات للمراجعة المنتظمة لسجلات أنشطة نظام المعلومات مثل سجلات المراجعة وتقارير الدخول وتقارير تتبع الحوادث الأمنية
164.308(a)(2)	(i) إسناد المسؤولية الأمنية. تحديد مسئول الأمن والذي سيكون مسئول عن وضع وتنفيذ السياسات والإجراءات المطلوبة من هذا القسم الفرعي للكيان	(مطلوب)

تابع الجدول رقم (١٠٤,١).

الضمانات الإدارية		
القسم	المعايير	مواصفات التنفيذ
164.308(a)(3)	(i) أمن القوى العاملة. تنفيذ سياسات وإجراءات لضمان أن لجميع أفراد القوة العاملة لدى المؤسسة صلاحية الدخول المناسبة للمعلومات الصحية الإلكترونية المحمية على النحو المنصوص عليه في الفقرة (4)(a) من هذا المقطع، ومنع أعضاء القوى العاملة الذين ليس لديهم صلاحية وصول بموجب الفقرة (4)(a) من هذا المقطع من الوصول إلى المعلومات الصحية الإلكترونية المحمية	(A) ترخيص و/أو إشراف (قابل للمعالجة). تنفيذ إجراءات منح الترخيص (و/أو الإشراف على) لأعضاء من القوى العاملة الذين يعملون مع المعلومات الصحية الإلكترونية المحمية أو في المواقع التي يمكن فيها الوصول إلى هذه المعلومات (B) عملية التصريح للقوى العاملة (قابل للمعالجة). تنفيذ إجراءات لتحديد الدخول المناسب لأعضاء القوى العاملة إلى المعلومات الصحية الإلكترونية المحمية (C) إجراءات الإنهاء (قابل للمعالجة). تنفيذ إجراءات لإنهاء إمكانية الدخول إلى المعلومات الصحية الإلكترونية المحمية عند انتهاء توظيف أحد أعضاء القوى العاملة أو على النحو المطلوب في القرارات التي تتخذ على النحو المحدد في الفقرة (3)(ii)(B)(a) من هذه المادة.
164.308(a)(4)	(i) إدارة الدخول إلى المعلومات. تنفيذ سياسات وإجراءات لمنح تصريح الدخول إلى المعلومات الصحية الإلكترونية المحمية والتي تنسجم مع المتطلبات المعمول بها في القسم الفرعي E من هذا الجزء	(A) عزل وظائف مراكز تبادل معلومات الرعاية الصحية (مطلوب). إذا كان مركز تبادل المعلومات الرعاية الصحية هو جزء من منظمة أكبر فيجب على هذا المركز تنفيذ السياسات والإجراءات التي تحمي المعلومات الصحية الإلكترونية المحمية لهذا المركز من الوصول غير المصرح به من جانب المنظمة الأكبر. (B) تصريح الدخول (قابل للمعالجة). تنفيذ سياسات وإجراءات لمنح الدخول إلى المعلومات الصحية الإلكترونية المحمية، على سبيل المثال، من خلال الدخول إلى محطة العمل والمعاملات والبرنامج والعمليات أو أي آلية أخرى. (C) تأسيس الدخول والتعديل (قابل للمعالجة). تنفيذ السياسات والإجراءات (استنادا إلى سياسات تصريح الدخول للكيان) التي تضع وتوثق وتُراجع وتعدِّل حق المستخدم في الوصول إلى محطة العمل أو المعاملات أو البرامج أو العمليات.
164.308(a)(5)	(i) التوعية والتدريب بخصوص الأمن. تنفيذ برنامج التوعية والتدريب بخصوص الأمن لجميع أعضاء قوة العمل (بما في ذلك الإدارة)	(A) رسائل تذكرية بالأمن (قابل للمعالجة). التحديثات الأمنية الدورية. (B) الحماية من البرمجيات الخبيثة (قابل للمعالجة). إجراءات للحماية من البرامج الخبيثة وكشفها والإبلاغ عنها. (C) مراقبة تسجيل الدخول (قابل للمعالجة). إجراءات لمراقبة محاولات الدخول وتقديم تقارير بالتناقضات. (D) إدارة كلمة المرور السرية (قابل للمعالجة). الإجراءات اللازمة لإنشاء وتغيير وحماية كلمات المرور السرية.
164.308(a)(6)	(i) إجراءات حوادث الأمن. تنفيذ سياسات وإجراءات لمعالجة الحوادث الأمنية	الاستجابة والإبلاغ (مطلوب). تحديد الحوادث المشتبه بها أو الحوادث الأمنية والتجاوب معها وتخفيف (بالقدر الممكن عملياً) الآثار الضارة الناجمة عن الحوادث الأمنية والمعروفة للكيان المشمول وتوثيق حوادث الأمن ونتائجها.

تابع الجدول رقم (١,١٠٤).

الضمانات الإدارية		
القسم	المعايير	مواصفات التنفيذ
164.308(a)(7)	(i) خطة الطوارئ. إنشاء (وتنفيذ حسب الحاجة) سياسات وإجراءات للاستجابة لأي حالة طارئة أو أي حادثة أخرى (على سبيل المثال، تتسبب الحرائق والتخريب وفشل النظام والكوارث الطبيعية) بتخريب الأنظمة التي تحتوي على المعلومات الصحية الإلكترونية المحمية	(A) خطة النسخ الاحتياطي للبيانات (مطلوب). وضع وتنفيذ إجراءات لإنشاء نسخ دقيق للمعلومات الصحية الإلكترونية المحمية والحفاظ عليها. (B) خطة التعافي من الكوارث (مطلوب). إنشاء (وتنفيذ حسب الحاجة) إجراءات لاستعادة أية خسارة للبيانات. (C) خطة عمليات وضع الطوارئ (مطلوب). تأسيس (وتنفيذ حسب الحاجة) الإجراءات التي تُمكن من استمرار عمليات الأعمال الهامة لحماية أمن المعلومات الصحية الإلكترونية المحمية في حين التشغيل في وضع الطوارئ. (D) إجراءات الاختبار والتنقيح (قابل للمعالجة). تنفيذ إجراءات الاختبار الدوري والتنقيح لخطط الطوارئ. (E) تحليل التطبيقات وخطورة البيانات (قابل للمعالجة). تقييم نسبي لخطورة تطبيقات وبيانات محددة في دعم لعناصر أخرى في خطة الطوارئ.
164.308(a)(8)	(i) التقييم. تنفيذ تقييم تقني دوري وغير دوري (يعتمد في البداية على المعايير المنفذة بموجب هذه اللائحة، وبعد ذلك استجابة إلى التغيرات البيئية أو التشغيلية التي تؤثر على أمن المعلومات الصحية الإلكترونية المحمية) والذي يُحدد مدى تلبية السياسات والإجراءات الأمنية للكيان لمتطلبات هذا القسم الفرعي.	(مطلوب)

تابع الجدول رقم (١٠٤,١).

الضمانات الإدارية		
القسم	المعايير	مواصفات التنفيذ
164.308(b)	(1) عقود شركاء العمل والترتيبات الأخرى.قد يسمح الكيان المشمول (وفقاً للقسم 164.306) لشريك العمل بإنشاء أو تلقي أو المحافظة على أو نقل المعلومات الصحية الإلكترونية المحمية نيابة عن الكيان المشمول فقط إذا حصل الكيان المشمول على ضمانات مرضية (وفقاً للقسم 164.314(a)) بأن شريك العمل سوف يحمي هذه المعلومات. (2) لا ينطبق هذا المعيار فيما يتعلق بـــ (i) نقل المعلومات الصحية الإلكترونية المحمية من قبل الكيان المشمول إلى مُزود الرعاية الصحية بشأن معالجة شخصٍ ما. (ii) نقل المعلومات الصحية الإلكترونية المحمية من قبل مجموعة خطة الصحة أو HMO أو مُصدر التأمين الصحي نيابةً عن مجموعة خطة الصحة أو إلى راعي الخطة، إلى الحد الذي تنطبق فيه متطلبات القسمين 164.314(b) و164.504(f) ويتم استيفائها (iii) نقل المعلومات الصحية الإلكترونية المحمية من أو إلى وكالاتٍ أخرى توفر الخدمات بموجب القسم 164.502(e)(1)(ii)(C) عندما يكون الكيان المشمول هو خطة صحية لبرنامج حكومي يوفر منافع عامة، إذا تم استيفاء متطلبات القسم 164.502(e)(1)(ii)(C). (3) الكيان المشمول الذي ينتهك الضمانات المرضية التي قُدمت له كشريك عمل لكيان مشمول آخر سيكون في وضع عدم امتثال مع معايير ومواصفات التنفيذ ومتطلبات هذه الفقرة و 164.314(a).	عقد مكتوب أو ترتيبات أخرى (مطلوب). توثيق الضمانات المرضية المطلوبة بموجب الفقرة (b)(1) من هذا القسم من خلال عقد مكتوب أو ترتيبات أخرى مع شريك العمل يفي بمتطلبات القسم 164.314(a) المنطبقة.

تابع الجدول رقم (١٠٤,١).

الضمانات المادية		
القسم	المعايير	مواصفات التنفيذ
164.310(a)	(1) ضوابط الوصول إلى المنشأة. تنفيذ سياسات وإجراءات للحد من الوصول المادي إلى أنظمة المعلومات الإلكترونية والمنشأة أو المنشآت التي توجد فيها هذه الأنظمة مع ضمان سماح الوصول المصرح بشكلٍ صحيح	(i) عمليات الطوارئ (قابل للمعالجة). وضع (وتنفيذ حسب الحاجة) الإجراءات التي تتيح الوصول إلى المنشأة في دعم لاستعادة البيانات المفقودة في إطار خطة التعافي من الكوارث وخطة عمليات وضع الطوارئ في حال حدوث الطوارئ. (ii) خطة أمن المنشأة (قابل للمعالجة). تنفيذ سياسات وإجراءات لحماية المنشأة والتجهيزات التي فيها من الوصول المادي غير المصرح به والتلاعب والسرقة. (iii) إجراءات ضبط الوصول والتحقق من صحته (قابل للمعالجة). تنفيذ إجراءات لضبط وصول المستخدم إلى المنشأة والتحقق من صحة هذا الوصول على أساس دور أو وظيفة المستخدم، بما في ذلك ضبط الزائرين وضبط الوصول إلى برامج الكمبيوتر من أجل اختبارها وتنقيحها. (iv) سجلات الصيانة (قابل للمعالجة). تنفيذ سياسات وإجراءات لتوثيق الإصلاحات والتعديلات على المكونات المادية للمنشأة التي تتصل بالأمن (على سبيل المثال، التجهيزات والجدران والأبواب والأقفال).
164.310(b)	استخدام محطة العمل. تنفيذ السياسات والإجراءات التي تحدد الوظائف المناسبة التي يتعين القيام بها وطريقة القيام بتلك الوظائف والصفات المادية لمحطة عمل معينة محيطة أو فئة معينة من محطات العمل التي يمكنها الوصول إلى المعلومات الصحية الإلكترونية المحمية	(مطلوب)
164.310(c)	أمن محطة العمل. تنفيذ الضمانات المادية لجميع محطات العمل التي تصل إلى المعلومات الصحية الإلكترونية المحمية لتقييد الوصول على المستخدمين المخولين فقط	(مطلوب)
164.310(d)	(1) ضبط الأجهزة والوسائط. تنفيذ السياسات والإجراءات التي تحكم تلقي وإزالة الأجهزة والوسائط الإلكترونية التي تحتوي المعلومات الصحية الإلكترونية المحمية داخل وخارج المنشأة وحركة هذه المواد ضمن المنشأة	(i) الإتلاف (مطلوب). تنفيذ سياسات وإجراءات لمعالجة التخلص النهائي من المعلومات الصحية الإلكترونية المحمية و/أو الأجهزة أو الوسائط الإلكترونية التي تُخزن فيها هذه المعلومات. (ii) إعادة استخدام الوسائط (مطلوب). تنفيذ إجراءات إزالة المعلومات الصحية الإلكترونية المحمية من الوسائط الإلكترونية قبل إتاحة هذه الوسائط لإعادة الاستخدام. (iii) المسئولية (قابل للمعالجة). الاحتفاظ بسجل لتحركات الأجهزة والوسائط الإلكترونية وأي شخص مسئول عن ذلك. (iv) النسخ الاحتياطي وتخزين البيانات (قابل للمعالجة). إنشاء نسخة مطابقة تماماً للمعلومات الصحية الإلكترونية المحمية قابلة للاسترجاع عند الحاجة وذلك قبل نقل الأجهزة.

تابع الجدول رقم (١٠٤,١).

الضمانات الفنية		
القسم	المعايير	مواصفات التنفيذ
164.312(a)	(1) ضبط الدخول. تنفيذ السياسات والإجراءات التقنية اللازمة على أنظمة المعلومات الإلكترونية التي تحتفظ بالمعلومات الصحية الإلكترونية المحمية للسماح فقط بوصول الأشخاص الذين مُنحوا حق الوصول على النحو المحدد في القسم 164.308(a)(4)	(i) تعرُّف فريد على المستخدم (مطلوب). تعيين اسم و/أو رقم فريد لتحديد وتتبع هوية المستخدم. (ii) عملية الدخول في حالات الطوارئ (مطلوب). إنشاء الإجراءات اللازمة (وتنفيذها حسب الحاجة) للحصول على المعلومات الصحية الإلكترونية المحمية الضرورية في حالة الطوارئ. (iii) الخروج التلقائي (قابل للمعالجة). تنفيذ إجراءات إلكترونية تُنهي الجلسة الإلكترونية بعد زمن خمول محددة مسبقاً. (iv) التشفير وفك التشفير (قابل للمعالجة). تنفيذ آلية لتشفير وفك تشفير المعلومات الصحية الإلكترونية المحمية.
164.312(b)	مراجعة الضوابط. تنفيذ الأجهزة والبرامج و/أو الآليات الإجرائية التي تسجل وتفحص النشاط في أنظمة المعلومات التي تحتوي على المعلومات الصحية الإلكترونية المحمية أو تستخدمها	(مطلوب)
164.312(c)	(1) النزاهة. تنفيذ سياسات وإجراءات لحماية المعلومات الصحية الإلكترونية المحمية من التحريف غير اللائق والتخريب	(2) آلية للمصادقة على صحة المعلومات الصحية الإلكترونية المحمية (قابل للمعالجة). تنفيذ آليات إلكترونية لإثبات عدم تغيير أو تخريب المعلومات الصحية الإلكترونية المحمية بطريقة غير مشروعة.
164.312(d)	المصادقة على الشخص أو الكيان. تنفيذ إجراءات للتحقق من أن الشخص أو الكيان الذي يسعى إلى الوصول إلى المعلومات الصحية الإلكترونية المحمية هو الشخص أو الكيان الصحيح	(مطلوب)
164.312(e)	(1) أمن النقل. تنفيذ تدابير أمنية تقنية للحماية من الوصول غير المصرح به إلى المعلومات الصحية الإلكترونية المحمية التي يجري نقلها عبر شبكة اتصالات إلكترونية.	(i) ضوابط النزاهة (قابل للمعالجة). تنفيذ تدابير أمنية لضمان عدم التعديل غير الصحيح للمعلومات الصحية الإلكترونية المحمية التي يتم نقلها إلكترونياً من دون كشف هذا التعديل حتى يتم التخلص من هذه المعلومات. (ii) التشفير (قابل للمعالجة). تنفيذ آلية لتشفير المعلومات الصحية الإلكترونية المحمية كلما كان ذلك مناسباً.

تابع الجدول رقم (١٠٤,١).

الضمانات التنظيمية		
القسم	المعايير	مواصفات التنفيذ
164.314(a)	(1) عقود شركاء العمل أو ترتيبات أخرى (i) يجب أن يستوفي العقد (أو ترتيب آخر) بين الكيان المشمول وشركاء العمل المطلوب بالقسم 164.308(b) الشروط الواردة في الفقرة (a)(2)(i) أو الفقرة (a)(2)(ii) من هذا الباب حسب المقتضى. (ii) لا يكون الكيان المشمول في امتثال مع المعايير الواردة في القسم 164.502(e) والفقرة (A) من هذا القسم إذا كان على معرفة بوجود نمط من النشاط أو الممارسة من قبل شركاء العمل يشكل انتهاكاً وخرقاً مادياً لالتزام شريك العمل بموجب العقد أو الترتيبات الأخرى، ما لم يتخذ الكيان المشمول خطوات معقولة لعلاج هذا الانتهاك أو إنهاء هذا الخرق حسب المقتضى، وإذا كانت مثل هذه الخطوات غير ناجحة:	(i) عقود شركاء العمل (مطلوب). يجب أن ينص العقد المبرم بين الكيان المشمول والشريك أن الشريك التجاري سوف– (A) يُنفذ الضمانات الإدارية والمادية والتقنية التي تحمي وبشكلٍ معقول ومناسب نزاهة وتوافر المعلومات الصحية الإلكترونية المحمية التي يُنشئها أو يتلقاها أو يحتفظ بها أو ينقلها بالنيابة عن الكيان المشمول على النحو المطلوب في هذا القسم الفرعي، (B) يضمن موافقة أي وكيل (بما في ذلك المتعاقد الثانوي) يُقدم له مثل هذه المعلومات على تنفيذ ضمانات معقولة ومناسبة لحماية هذه المعلومات، (C) يُقدم تقرير إلى الكيان المشمول عن أي حادث أمني أصبح على علم فيه (D) يُخول الكيان المشمول بإنهاء العقد إذا حدد الكيان المشمول أن شريك العمل قد انتهك مادة من مواد العقد. (ii) ترتيبات أخرى. (مطلوب) (A) إذا كان كلاً من الكيان المشمول وشريك العمل كيانين حكوميين فإن الكيان المشمول يكون في امتثال مع الفقرة (a)(1) من هذا الباب إذا– (١) دخل في مذكرة تفاهم مع شريك العمل تحتوي على البنود التي تُحقق الأهداف الواردة في الفقرة (a)(2)(i) من هذا الباب أو (٢) قانون أخر (بما في ذلك الأنظمة المعتمدة من قبل الكيان المشمول أو شريك العمل) يحتوي على متطلبات تنطبق على شريك العمل تُحقق الأهداف الواردة في الفقرة (a)(2)(i) من هذا الباب. (B) إذا كان مطلوباً من شريك العمل بموجب القانون أداء وظيفة ما أو نشاط ما نيابةً عن الكيان المشمول أو تقديم خدمة موصوفة في تعريف شريك العمل إلى الكيان المشمول على النحو المحدد في القسم 160.103 من هذا الفصل الفرعي، فقد يسمح الكيان المشمول لشريك العمل بإنشاء وتلقي والحفاظ على أو نقل المعلومات الصحية الإلكترونية المحمية نيابةً عنه بالقدر اللازم للامتثال بالمتطلب القانوني دون تحقيق متطلبات الفقرة (a)(2)(i) من هذا القسم، شريطة أن يُحاول الكيان المشمول وبحسن نية الحصول على ضمانات مُرضية كما هو مطلوب من (a)(2)(ii)(A) من هذا الباب، وأن يوثق هذه المحاولة وأسباب عدم إمكانية الحصول على هذه التأكيدات. (C) قد يحذف الكيان المشمول من ترتيباته الأخرى تخويل إنهاء العقد من قبل الكيان المشمول، كما هو مطلوب بموجب الفقرة (a)(2)(i)(D) من هذه المادة إذا كان مثل هذا التخويل لا يتسق مع الالتزامات النظامية للكيان المشمول أو لشريك العمل.
(A)	فسخ العقد أو الترتيبات إذا كان ذلك ممكناً أو	
(B)	إذا كان الفسخ أمراً غير ممكن فيجب تقديم تقرير بالمشكلة إلى أمين السر	

تابع الجدول رقم (١٠٤,١).

الضمانات التنظيمية		
القسم	المعايير	مواصفات التنفيذ
164.314(b)	(1) متطلبات من أجل الخطط الصحية الجماعية. فقط ما عدا الحالة التي يتم فيها كشف المعلومات الصحية الإلكترونية المحمية إلى راعي الخطة عملاً بالقسم 164.504(f)(1)(ii) أو (iii) أو على النحو المأذون به بموجب القسم 164.508، فيجب أن تضمن الخطة الصحية الجماعية أن وثائق خطتها تُبين أن راعي الخطة سوف يحمي وبشكلٍ معقول ومناسب إنشاء أو تلقي أو الحفاظ على أو نقل المعلومات الصحية الإلكترونية المحمية إلى (أو من قِبَل) راعي الخطة نيابةً عن الخطة الصحية الجماعية	(2) (مطلوب) يجب تعديل وثائق الخطة للخطة الصحية الجماعية لإدراج الأحكام التي تقتضي من راعي الخطة أن يقوم بـ: (i) تنفيذ الضمانات الإدارية والمادية والتقنية التي تحمي وبشكلٍ معقول ومناسب سرية وسلامة وتوافر المعلومات الصحية الإلكترونية المحمية التي يُنشئها أو يتلقاها أو يحتفظ بها أو ينقلها بالنيابة عن الخطة الصحية الجماعية. (ii) ضمان دعم الفصل الكافي التي يتطلبه القسم 164.504(f)(2)(iii) من قبل التدابير الأمنية المعقولة والمناسبة، (iii) ضمان موافقة أي وكيل (بما في ذلك المتعاقد الثانوي) تُقدَّم له هذه المعلومات على تنفيذ الإجراءات الأمنية المعقولة والمناسبة لحماية المعلومات و (iv) تقدم تقرير إلى الخطة الصحية الجماعية عن أي حادث أمني يُصبح راعي الخطة على علم به.

السياسات والإجراءات ومُتطلبات التوثيق		
القسم	المعايير	مواصفات التنفيذ
164.316(a)	السياسات والإجراءات. تنفيذ السياسات والإجراءات المعقولة والمناسبة لتحقيق المعايير ومواصفات التنفيذ أو غيرها من متطلبات هذا القسم الفرعي مع الأخذ في الاعتبار تلك العوامل المحددة في القسم 164.306(b)(2)(i), (ii), (iii), (iv). لا ينبغي أن يُفسَّر هذا المعيار على أنه يُصرح أو يعذر أي عمل ينتهك أي معيار آخر أو مواصفات التنفيذ أو متطلبات أخرى في هذا القسم الفرعي. يمكن للكيان المشمول أن يُغير سياساته وإجراءاته في أي وقت شريطة توثيق التغييرات وتنفذها وفقاً لهذا القسم الفرعي.	(مطلوب)

تابع الجدول رقم (١٠٤,١).

السياسات والإجراءات ومتطلبات التوثيق		
القسم	المعايير	مواصفات التنفيذ
164.316(b)	(1) التوثيق (ii) إذا كان مطلوباً في هذا القسم الفرعي توثيق أي عمل أو نشاط أو تقييم، فيجب الحفاظ على سجل مكتوب (والذي قد يكون إلكتروني) لهذا العمل أو النشاط أو التقييم	(i) الحفاظ على السياسات والإجراءات المنفذة امتثالاً لهذا القسم الفرعي في شكلٍ كتابي (الذي قد يكون إلكتروني) (i) الحد الزمني (مطلوب). الإبقاء على الوثائق المطلوبة بموجب الفقرة (1)(b) من هذا الفرع لمدة ٦ سنوات من تاريخ إنشائها أو من آخر تاريخ كانت فيه سارية المفعول، أيهما أبعد. (ii) التوافر (مطلوب). جعل الوثائق متاحة لأولئك الأشخاص المسئولين عن تنفيذ الإجراءات التي تتعلق بالوثائق. (iii) التحديثات (مطلوب). مراجعة الوثائق بصفة دورية وتحديثها حسب الحاجة وذلك استجابة للتغيرات البيئية والتشغيلية التي تؤثر على أمن المعلومات الصحية الإلكترونية المحمية

(المطلوب "Required") مقابل (قابل للمعالجة "Addressable")

يجب على الكيان أن يقرر ما إذا كانت مواصفات التنفيذ (القابلة للمعالجة) تُمثل تدبيراً أمنياً معقولاً ومناسباً للتطبيق ضمن إطار العمل الأمني الخاص به. سوف يعتمد هذا القرار على مجموعة متنوعة من العوامل، مثل (من بين أمور أخرى) عوامل تحليل المخاطر وإستراتيجية التخفيف من المخاطر والتدابير الأمنية الموجودة بالفعل وتكلفة التنفيذ بالنسبة إلى الكيان. اعتماداً على هذا القرار فإنه سوف ينطبق ما يلي:

(أ) إذا تم تحديد أن مواصفة معينة من مواصفات التنفيذ (القابلة للمعالجة) هي معقولة ومناسبة فيجب على الكيان المشمول تنفيذها.

(ب) إذا تم تحديد أن مواصفة معينة من مواصفات التنفيذ (القابلة للمعالجة) تُمثل تدبيراً أمنياً غير مناسب و/أو غير معقولة للكيان المشمول ولكن لا يمكن تحقيق المعيار من دون تنفيذ حماية أمنية إضافية، فيمكن للكيان المشمول أن يُنفذ تدبيراً بديلاً يُحقق نفس النهاية التي تحققها مواصفات التنفيذ (القابل للمعالجة). يجب على الكيان الذي يُحقق معياراً معيناً من خلال تدابير بديلة توثيق قرار عدم تنفيذ المواصفات التنفيذ (القابل للمعالجة) والأساس المنطقي وراء هذا القرار والضمان البديل الذي تم تنفيذه لتلبية المعيار.

يجب على مُزود الرعاية الصحية المشمول أن يمتثل للمتطلبات المنطبقة في هذا القسم الفرعي (على سبيل المثال، جزء الأمن والخصوصية 164، القسم الفرعي C – المعايير الأمنية لحماية المعلومات الإلكترونية المحمية) في موعد أقصاه ٢٠ أبريل ٢٠٠٥

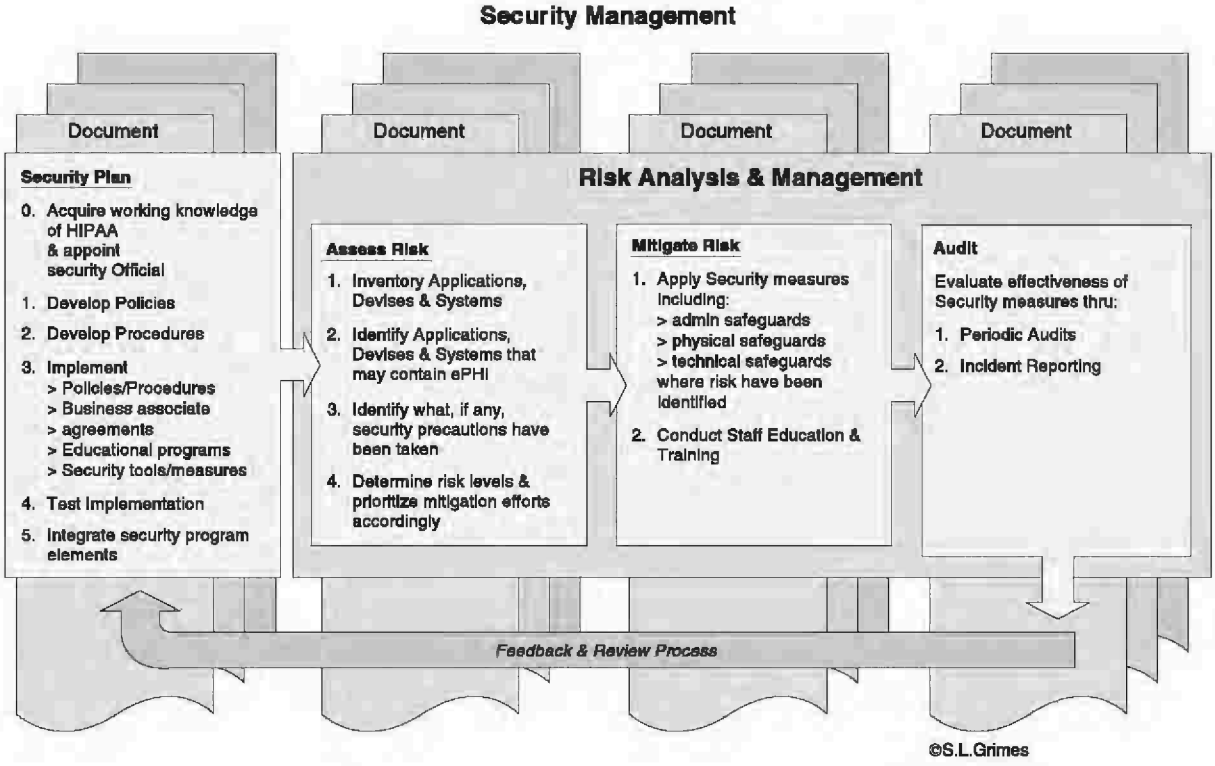
* إصلاح التأمين الصحي: معايير الأمن، اللائحة النهائية (68 FR 8334-8381 في ٢٠ فبراير ٢٠٠٣)

الجزء 164: الأمن والخصوصية، الجزء الفرعي C: المعايير الأمنية لحماية المعلومات الصحية الإلكترونية المحمية

عملية الامتثال
The Compliance Process

إدارة الأمن Security Management

تفرض اللائحة الأمنية لـ HIPAA على مقدمي الرعاية أن يقوموا بصياغة برنامج لإدارة الأمن ودمج عناصر تحليل وإدارة المخاطر في تلك العملية (انظر الشكل رقم ١٠٤,٤).



الشكل رقم (١٠٤,٤). إدارة الأمن وعملية تحليل وإدارة المخاطر وفقاً لـــ HIPAA.

من أجل تأسيس برنامج فعال لإدارة الأمن فيجب على كل مُنظمة أولاً أن تُعين مسئولاً أمنياً ذا سلطة ومسؤولية شاملة لتطوير وتنفيذ وإدارة التدابير الأمنية للمنظمة. يجب على مُزود الرعاية بعد تعيين المسئول الأمني التقدم في المستويات الخمسة للخطة الأمنية (انظر الشكل رقم ١٠٤,٥) من أجل تحقيق الهدف المتمثل في برنامج أمن فعال حقاً. تتضمن المستويات هذه ما يلي:

الشكل رقم (١٠٤,٥). مستويات إدارة الأمن للائحة الأمنية لـ HIPAA.

المستوى ١ (Level 1): وضع السياسات اللازمة لكل معيار من معايير اللائحة الأمنية.

يجب على كل منظمة تزويد للرعاية وضع مجموعة من السياسات التي تُصمم لتلبية المُتطلبات الخاصة باللائحة الأمنية التي تكون مُصممة أيضاً بحيث تُناسب شخصية المنظمة (أي وحجمها وتعقيدها وقدرتها). يجب على هذه السياسات أن تعالج قضايا مثل:

- إدارة الأمن.
- العقوبات.
- أمن القوى العاملة.
- إدارة الوصول إلى المعلومات.
- الحوادث الأمنية.
- التخطيط لحالات الطوارئ.
- اتفاقات شركاء العمل.
- التقييمات الدورية.
- ضوابط الدخول إلى المنشأة.
- استخدام الأجهزة/الأنظمة (أي الأنظمة التي تحافظ وتنقل الـ ePHI).
- الضوابط الأجهزة والوسائط (أي الأنظمة التي تحافظ وتنقل الـ ePHI).
- النزاهة (أي حماية الـ ePHI من التغيير أو التخريب).

- الاحتفاظ بالوثائق لمدة ٦ سنوات ومراجعتها وتحديثها دورياً.

المستوى ٢ (Level 2): وضع واعتماد الإجراءات اللازمة بما في ذلك الضمانات المادية والتقنية لكل مواصفة من مواصفات التنفيذ للائحة الأمنية.

بعد وضع السياسات (المناسبة للمؤسسة) التي تُعالج معايير اللائحة الأمنية فيجب على مقدم الرعاية وضع إجراءات تكميلية وضمانات مادية وتقنية لتتبع مواصفات التنفيذ للائحة الأمنية. تشمل الأمثلة على ذلك ما يلي:

- تحليل المخاطر وإدارة المخاطر وإجراءات مراجعة نشاط النظام من أجل معالجة سياسات إدارة الأمن.
- التصريح/الإشراف وترخيص القوى العاملة وإجراءات الإنهاء لمعالجة سياسات أمن القوى العاملة.
- تصريح الدخول وإجراءات إنشاء تأسيس/تعديل الدخول لمعالجة سياسات إدارة الدخول.
- التذكير الأمني ومراقبة الدخول وإجراءات إدارة الكلمة السرية للمرور لمعالجة سياسات الوعي الأمني.
- الاستجابة الأمنية وإجراءات الإبلاغ لمعالجة سياسات حوادث الأمن.
- النسخ الاحتياطي للبيانات والتعافي من الكوارث والتشغيل في نمط الطوارئ وإجراءات الاختبار لمعالجة سياسات خطة الطوارئ.
- إجراءات شركاء العمل لمعالجة سياسات شركاء العمل.
- إجراءات التقييم لمعالجة سياسات التقييم.
- عمليات الطوارئ وخطط أمن المنشأة وضبط الدخول والتحقق من الدخول والمحافظة على السجلات والضمانات المادية لمعالجة سياسات الوصول إلى المنشأة.
- إجراءات استخدام وأمن الأجهزة/الأنظمة والضمانات المادية لمعالجة سياسات استخدام وأمن النظام.
- إجراءات التخلص من البيانات وإعادة استخدام الوسائط وتعقب النظام/البيانات والحفظ الاحتياطي/التخزين للبيانات والضمانات المادية لمعالجة سياسات ضبط الأجهزة والوسائط.
- إجراءات تحديد هوية المستخدم والدخول الطارئ والخروج التلقائي والتشفير/فك التشفير لمعالجة سياسات ضبط الدخول.
- مراجعة إجراءات الرقابة والضمانات التقنية لمعالجة سياسات مراجعة الرقابة.
- إجراءات التحقق من البيانات والضمانات التقنية لمعالجة سياسات نزاهة البيانات.
- إجراءات ضبط النزاهة والتشفير والضمانات التقنية لمعالجة سياسات أمن النقل.
- إجراءات التوثيق لمعالجة سياسات التوثيق.

المستوى ٣ (Level 3): تنفيذ السياسات/الإجراءات والاتفاقات مع شركاء العمل وتعليم القوى العاملة والضمانات المادية/التقنية.

يجب على مُزود الرعاية بعد وضع السياسات والإجراءات والضمانات المادية والتقنية المُكملة والملائمة من أجل تلبية متطلبات اللوائح الأمنية أن يقوم بتنفيذ هذه التدابير على نحوٍ فعال.

المستوى ٤ (Level 4): اختبار التنفيذ.

يجب على مُزود الرعاية بعد تنفيذ السياسات والإجراءات والضمانات المادية والتقنية إجراء اختبار مستمر للتحقق من فعاليتها وتحديد التغييرات المطلوبة للحفاظ على فعالية هذه التدابير.

المستوى ٥ (Level 5): إدماج التدابير الأمنية في برنامج شامل للمنظمة.

أخيراً، يجب على مُزود الرعاية ضمان تكامل هذه التدابير في مُجمل عملياته وفي برامج الأمن. لا يمكن اعتبار أن برنامج إدارة الأمن فعالاً إلا بعد تحقيق هذا التكامل.

تحليل وإدارة المخاطر Risk Analysis and Management

تفرض اللائحة الأمنية أنه يجب على مُزود الرعاية بالتزامن مع عملية وضع خطة الأمن أن يقوم بإدراج عناصر تحليل وإدارة المخاطر في هذه العملية. تتضمن هذه العناصر بالنسبة إلى برامج التكنولوجيا الطبية الحيوية على ما يلي:

الجرد An Inventory

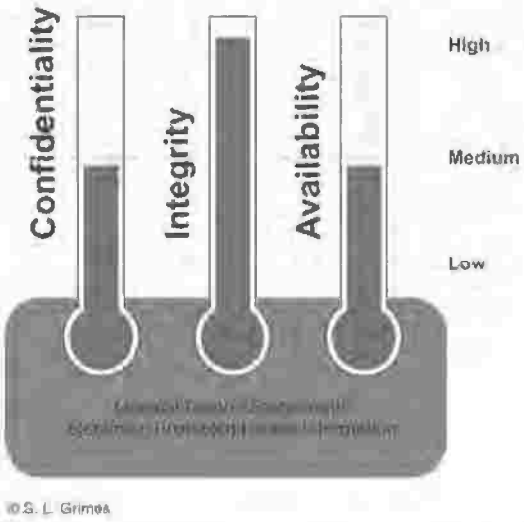
يجب على مزود الرعاية تحديد الأجهزة الطبية الحيوية والأنظمة التي تحتفظ/تنقل الـ ePHI. يجب على المنظمة عادةً أن تُجيب على الأسئلة التالية لكل جهاز/نظام ذو صلة:

- ما هو نوع (أو أنواع) الـ ePHI التي يقوم الجهاز/النظام باحتوائها؟
- من الذي لديه حق الوصول إلى الـ ePHI؟ من الذي يحتاج إلى الوصول إلى الـ ePHI ؟
- ما هي أنواع الاتصالات الموجودة مع الأجهزة/الأنظمة الأخرى؟
- ما هي أنواع التدابير الأمنية المُطبقة حالياً في هذا الجهاز/النظام؟

تقييم المخاطر المرتبطة بـ ePHI للأصناف المجرودة Assessing the Risk Associated with ePHI in Inventoried Items

يجب على مزود الرعاية أن يقون بتصنيف مستويات المخاطر فيما يتعلق باحتمال إضعاف سرية ونزاهة وتوافر الـ ePHI. يتحدد مستوى الخطر من خلال النظر إلى كل من درجة خطورة (أن تصبح الـ ePHI في خطر) واحتمال حدوث مثل هذا الخطر أو الإضعاف لـ ePHI (انظر الشكل رقم ١٠٤,٦).

- الخطورة: مستوى المخاطر/الضعف (على سبيل المثال، عالي أو متوسط أو منخفض) فيما يتعلق بسرية وسلامة ومدى توافر الـ ePHI لكل جهاز/نظام ذو صلة.
- الاحتمال: احتمال حدوث الخطر (على سبيل المثال، بشكلٍ متكرر أو عرضي أو نادر) فيما يتعلق بسرية وسلامة ومدى توافر الـ ePHI لكل جهاز/نظام ذو صلة.
- درجة الخطورة المُركبة: جمع مستوى الخطورة ومستوى الاحتمال في درجة خطورة مُركبة بالنسبة لكل جهاز ونظام يحتفظ أو ينقل الـ ePHI.



الشكل رقم (١٠٤,٦). مستويات الخطورة بالنسبة إلى سرية وسلامة وتوافر الـ ePHI للجهاز الطبي أو النظام ذي الصلة.

تحديد الأولويات Establishing Priorities

يمكن لمُزود الرعاية أن يستخدم الدرجات لتحديد الأولويات بعد وضع درجة خطورة مُركبة لكل جهاز ونظام يحتفظ أو ينقل الـ ePHI. يمكن لمُزود الرعاية أن:

- يستخدم علامات الخطورة/الاحتمال المُركبة لوضع أولويات جهود التخفيف من حدة المخاطر.
- يقوم بجهود التخفيف التي تعطي الأولوية للأجهزة والأنظمة التي لها أعلى الدرجات (أي الأجهزة/الأنظمة التي تمثل أهم المخاطر).
- تحديد الفجوة.

وفقا للأولويات المحددة لكل جهاز والنظام في قوائم الجرد:

- يجب مراجعة الإجراءات الأمنية الحالية التي تم تحديدها خلال عملية جرد الأجهزة الطبية الحيوية والأنظمة.

- يجب إعداد تحليل الفجوة بالنسبة للأجهزة وأنظمة تتضمن التدابير الأمنية الإضافية اللازمة للتخفيف من حدة المخاطر المعروفة (معالجة الأجهزة والأنظمة وفقاً للأولوية).

صياغة وتنفيذ خطة التخفيف Formulating and Implementing a Mitigation Plan

ينبغي بعد تحديد الفجوة بين التدابير الأمنية القائمة والمطلوبة وإعطاء أولويات للأجهزة والأنظمة وفقاً لمستويات المخاطر:

- إعداد خطة مكتوبة تتضمن:
- تدابير أمنية إضافية على النحو المطلوب.
- تقييم الأولويات.
- الجدول الزمني للتنفيذ.
- تنفيذ الخطة وتوثيق العملية.
- مراقبة العملية.

كما ينبغي التأكد من المراجعة المستمرة لعملية تحليل وإدارة المخاطر وتحسينها حسب الاقتضاء عن طريق:

- وضع أنظمة مراقبة مستمرة (بما في ذلك نظام الإبلاغ عن الحوادث الأمنية) لضمان فعالية الجهود الرامية إلى التخفيف.
- توثيق نتائج المراجعة المنتظمة للعمليات الأمنية.

الموجز
Summary

في حين أن عملية الامتثال المرتبطة باللائحة الأمنية لـ HIPAA قد تبدو مرهقة في البداية، إلا أن الـ HIPAA لم يضع الكثير من أعباء الامتثال الإضافية على المهندسين الإكلينيكيين بل شرَّع عناصر رئيسية عديدة للهندسة الإكلينيكية الفعالة أو لبرنامج إدارة التكنولوجيا الطبية الحيوية. يجب أن نتذكر أن أحكام التبسيط الإداري لـ HIPAA تتعلق أولاً وقبل كل شيء بالمعايير. تقوم المعايير في هذه الحالة بتسهيل التبادل السريع والدقيق للمعلومات ذات الصلة بالمريض فيما بين مقدمي الرعاية وشركات التأمين وغيرهم من المشاركين في عمليات الرعاية الصحية. تفرض اللائحة الأمنية لـ HIPAA أن يضمن مقدمو الرعاية سلامة وتوافر وسرية المعلومات ذات الصلة بالمريض بما في ذلك البيانات التشخيصية والعلاجية. يجب أن نعتبر أن ضمان سلامة وتوافر البيانات في الأجهزة والأنظمة التشخيصية والعلاجية هو هدف مبدأي وجوهري لأي برنامج فعال للهندسة الإكلينيكية. تُعطي اللائحة الأمنية هذا الهدف قوة القانون كما أنها تُضيف اعتبارات السرية.

يُعتبر HIPAA قوة رئيسية في التنمية المستقبلية لنظام الرعاية الصحية في الولايات المتحدة وعلى هذا النحو فإنه سيكون مجال تركيز معظم مسئولي الرعاية الصحية والمخططين لسنوات عديدة. ينبغي على المهندسين الإكلينيكيين أن يُدركوا فرصتهم للمساهمة في سبل معالجة هذه المسألة.

المراجع

References

Duncan M, Rishel W, Kleinberg K, et al. A Common Sense Approach to HIPAA. , GartnerGroup, March 2001.

45 CFR Parts 160, 162 and 164.Federal Register 68(34) , 2003. 45 CFR Parts 160, 162 and 164.

Heffler S et al. Trends: Health Spending Projections For 2002-2012. Health Affairs W3:54-65, 2003.

Lageman RC, Melick JR. HIPAA: Wake-Up Call for Health Care Providers. Fitch IBCA, Duff and Phelps, 2000.

Marietti C. Beyond Y2K. Health Care Informatics 11: , 1999.

Moynihan JJ. The Basics of HIPAA for Clinicians, Health Care Executives and Trustees, Compliance Officers, Privacy Officers, and Legal Counsel. First National HIPAA Summit. 2000.

Woolhandler S, Himmelstein DU. The Deteriorating Administrative Efficiency of the U.S. Health Care System. New England Journal of Medicine 324:1253-1258, 1991.