



الدورة التدريبية: أمن المعلومات في الرعاية الصحية - حماية بيانات المرضى والامتثال

13 - 17 ديسمبر 2026

اسطنبول

(للشخص الواحد) € 4900

Ref: #CYB7673_397321



مقدمة الدورة التدريبية / لمحة عامة:

يمثل أمن المعلومات في الرعاية الصحية تحديًا بالغ الأهمية نظرًا للحساسية القصوى لبيانات المرضى والسجلات الطبية الإلكترونية. هذه الدورة التدريبية المتخصصة مصممة خصيصًا للمهنيين العاملين في القطاع الصحي، بهدف تزويدهم بالمعرفة والمهارات اللازمة لحماية بيانات المرضى وضمان الامتثال للوائح الصحية الصارمة. سنتناول في هذه الدورة مبادئ حماية بيانات الرعاية الصحية، أطر عمل الامتثال مثل HIPAA وGDPR، واستراتيجيات الوقاية من اختراق البيانات الصحية. سيكتسب المشاركون فهمًا عميقًا للتهديدات السيبرانية التي تواجه المستشفيات والمرافق الصحية، وكيفية تطبيق أفضل الممارسات الأمنية لتأمين البنية التحتية الصحية. تهدف الدورة إلى تمكين العاملين في القطاع الصحي من بناء بيئة معلوماتية آمنة وموثوقة، مع الحفاظ على سرية وسلامة وتوافر بيانات المرضى. يستند المحتوى إلى أحدث المعايير الدولية والوطنية لأمن المعلومات الصحية، مع الإشارة إلى مساهمات خبراء أكاديميين بارزين مثل البروفيسور دانيال سولوف (Daniel Solove)، أحد أبرز المتخصصين في قوانين الخصوصية وحماية البيانات. يقدم BIG BEN Training Center هذه الدورة لتعزيز الوعي الأمني والامتثال التنظيمي في قطاع الرعاية الصحية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو تكنولوجيا المعلومات في المستشفيات والمراكز الصحية.
- متخصصو أمن المعلومات في قطاع الرعاية الصحية.
- المسؤولون عن الامتثال التنظيمي وحماية البيانات الصحية.
- الأطباء والممرضون والإداريون المتعاملون مع السجلات الطبية الإلكترونية.
- مدققو الأنظمة الصحية.
- أخصائيو السجلات الطبية.

القطاعات والصناعات المستهدفة:

- المستشفيات والعيادات والمراكز الطبية.
- شركات التأمين الصحي وشركات إدارة المطالبات.
- مختبرات التحاليل الطبية والصيديات.
- شركات تطوير البرمجيات وأنظمة المعلومات الصحية.
- الهيئات الحكومية وما في حكمها، خاصة تلك المعنية بتنظيم الرعاية الصحية وحماية البيانات.
- شركات الأجهزة الطبية التي تتصل بالشبكة.



الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة أمن المعلومات.
- إدارة الجودة والامتثال.
- الإدارة الطبية والإدارة التمريضية.
- قسم السجلات الطبية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم أهمية أمن المعلومات وخصوصية بيانات المرضى في الرعاية الصحية.
- التعرف على اللوائح والمعايير الرئيسية لأمن البيانات الصحية (مثل HIPAA, GDPR).
- تطبيق أفضل الممارسات لحماية السجلات الطبية الإلكترونية.
- القدرة على تحديد التهديدات السيبرانية الشائعة التي تواجه المؤسسات الصحية.
- وضع سياسات وإجراءات أمنية لحماية بيانات المرضى.
- التعامل مع حوادث اختراق البيانات الصحية والاستجابة لها.
- تعزيز ثقافة الوعي الأمني بين العاملين في الرعاية الصحية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتفاعلية، مصممة خصيصًا لمواجهة التحديات الفريدة لأمن المعلومات في الرعاية الصحية. سيتمكن المشاركون من خلال دراسات الحالة الواقعية لاخترافات البيانات الصحية، وورش العمل التطبيقية، من فهم كيفية تطبيق مبادئ الأمن السيبراني في بيئة العمل اليومية. تتضمن المنهجية مناقشات تفاعلية حول الامتثال للوائح مثل HIPAA وGDPR، وكيفية تنفيذ الضوابط الأمنية اللازمة. سيتم التركيز على أمن الأجهزة الطبية المتصلة بالشبكة، وحماية الأنظمة السحابية المستخدمة في الرعاية الصحية. يقدم BIG BEN Training Center هذه الدورة لتمكين المتخصصين في القطاع الصحي من حماية بيانات المرضى بفعالية وتعزيز مرونة مؤسساتهم ضد التهديدات السيبرانية.



خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات وخصوصية بيانات المرضى

- مقدمة إلى أمن المعلومات في الرعاية الصحية.
- أهمية خصوصية بيانات المرضى وسرية السجلات الطبية.
- التهديدات السيبرانية الفريدة التي تواجه القطاع الصحي.
- مخاطر اختراق البيانات الصحية على المؤسسات والأفراد.
- مبادئ أمن المعلومات: السرية، السلامة، التوافر.
- أنواع البيانات الصحية الحساسة.
- تأثير اختراق بيانات المرضى.

الوحدة الثانية: اللوائح والمعايير الرئيسية لأمن البيانات الصحية

- قانون HIPAA (Health Insurance Portability and Accountability Act) ومتطلباته.
- اللائحة العامة لحماية البيانات (GDPR) وتأثيرها على القطاع الصحي.
- معايير ISO 27001 وتطبيقها في الرعاية الصحية.
- متطلبات الامتثال الأخرى ذات الصلة.
- إدارة المخاطر لأمن المعلومات الصحية.
- إعداد سياسات أمن المعلومات المخصصة للرعاية الصحية.
- التدقيق والتقييم الدوري للأمن.

الوحدة الثالثة: حماية السجلات الطبية الإلكترونية وأنظمة الرعاية الصحية

- تأمين السجلات الطبية الإلكترونية (EHR/EMR).
- أمن الشبكات في المستشفيات والمرافق الصحية.
- تشفير البيانات الصحية أثناء النقل والتخزين.
- إدارة الهوية والوصول (IAM) في البيئات السريرية.
- أمن الأجهزة الطبية المتصلة بالشبكة (IoT in Healthcare).
- حماية البيانات في الخدمات السحابية الصحية.
- أمن تطبيقات الرعاية الصحية.



الوحدة الرابعة: الاستجابة للحوادث الأمنية وإدارة الأزمات في الرعاية الصحية

- وضع خطة الاستجابة للحوادث الأمنية الصحية.
- اكتشاف الحوادث الأمنية في الأنظمة الصحية.
- التعامل مع اختراق بيانات المرضى والإبلاغ عنه.
- التحقيق الجنائي الرقمي في الحوادث الصحية.
- استمرارية الأعمال والتعافي من الكوارث في الرعاية الصحية.
- إدارة سمعة المؤسسة بعد الحوادث الأمنية.
- التواصل الفعال أثناء الأزمات الصحية.

الوحدة الخامسة: الوعي الأمني وبناء ثقافة أمنية في الرعاية الصحية

- برامج تدريب الوعي الأمني للعاملين في الرعاية الصحية.
- أهمية الثقافة الأمنية في الوقاية من الحوادث.
- أفضل الممارسات لسلامة الموظفين وتجنب الهندسة الاجتماعية.
- التحديات الأمنية للأجهزة المحمولة في الرعاية الصحية.
- التعاون مع الجهات الخارجية والجهات التنظيمية.
- الاستثمار في تقنيات الأمن الحديثة للرعاية الصحية.
- التحسين المستمر لبرنامج أمن المعلومات الصحي.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.



سؤال للتأمل:

في ظل التطور التكنولوجي السريع في الرعاية الصحية، والذي يشمل الذكاء الاصطناعي والأجهزة المتصلة، كيف يمكن للمؤسسات الصحية أن تحقق توازنًا دقيقًا بين تبني هذه الابتكارات لتعزيز رعاية المرضى وضمان أقصى درجات أمن المعلومات وخصوصية بيانات المرضى في آن واحد؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على أمن المعلومات في الرعاية الصحية، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الفريدة لهذا القطاع الحساس. بدلاً من المفاهيم العامة، نغوص في اللوائح والمعايير المحددة مثل HIPAA وGDPR، وكيفية تطبيقها عملياً لحماية بيانات المرضى. تقدم الدورة دراسات حالة واقعية لاختراقات البيانات الصحية، مع تحليل مفصل لنتائجها وكيفية الوقاية منها. نركز على بناء ثقافة أمنية قوية داخل المؤسسات الصحية، وتمكين العاملين من أن يصبحوا خط الدفاع الأول ضد التهديدات السيبرانية. إنها ليست مجرد دورة لتعلم الأساسيات، بل هي برنامج تدريبي شامل يهدف إلى بناء قدرات أمنية متقدمة لضمان سلامة وخصوصية بيانات المرضى في بيئة الرعاية الصحية المتغيرة.