Cybersecurity - IT-Sicherheit für Medizinprodukte.

Cybersicherheit für Ihre Medizinprodukte - Regulatory Cybersecurity Affairs sicherstellen.

Seminar | 7 Termine verfügbar | Teilnahmebescheinigung

Präsenz / Virtual Classroom | 8 Unterrichtseinheiten | Online durchführbar

Seminarnummer: 09540

Stand: 28.10.2025. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/09540

In der Medizintechnik ist Cybersecurity ein wichtiger Faktor und hat entscheidenden Einfluss auf die Sicherheit aktiver und insbesondere vernetzter Medizinprodukte. Der regulatorische Rahmen für die Cybersecurity (IT-Sicherheit) von Medizinprodukten wird für die EU im Abschnitt "Grundlegende Sicherheits- und Leistungsanforderungen" von MDR (EU) 2017/745 und IVDR (EU) 2017/746 vorgegeben. Normen und Leitlinien konkretisieren die Vorgaben für die Umsetzung. Im Bereich der FDA gibt es entsprechende Guidelines. Erfahren Sie u.a., wie Sie die CIA-Triade Vertraulichkeit, Integrität und Verfügbarkeit erreichen und Cybersecurity über den gesamten Produktlebenszyklus anforderungskonform sicherstellen.

Nutzen

- Sie kennen die regulatorischen und normativen Vorgaben an Cybersecurity von Medizinprodukten sowie die anzuwendenden Leitlinien.
- Sie erwerben Kenntnisse, wie Sie Ihre Entwurfs- und Herstellungsprozesse gestalten müssen, um Cybersicherheit über den Produktlebenszyklus sicherzustellen.
- Sie erwerben Kenntnisse über die Durchführung der notwendigen Risiko-Management-Maßnahmen, um Cybersecurity-Risiken zu mindern.
- Sie profitieren von konkreten Umsetzungsbeispielen aus der Praxis, die Ihnen die Implementierung bzw. Umsetzung erleichtern.

Zielgruppe

Personen aus Unternehmen, die Medizinprodukte herstellen, welche Software enthalten und netzwerkfähig sind, aus den Bereichen:

- Regulatory and Quality Affairs

- Risikomanagement
- Requirements Engineering
- Projekt- und Produktmanagement
- Software-Engineering
- IT-Management
- Dienstleister und Zulieferer

Inhalte des Seminars

- Cybersecurity von Medizinprodukten - Einführung
  - Grundlagen und Begriffe
  - Safety & Security
  - Schutzziele, Gefahren & Abwehr
  - Regulatory Cybersecurity Affairs – Was ist das und warum ist es wichtig für Hersteller von Medizinprodukten?
- Regulatorische und normative Anforderungen an die IT-Sicherheit von Medizinprodukten
  - Regularien (MDR, IVDR, MDCG-2019-16, MPBetreibV, FDA)
  - Normen und Leitlinien (IEC 81001-5-1, IEC 62443-4-1, ISO/IEC 27001, IEC 60606-1, IEC 80001-1 für Hersteller, ISO 27034, AMI TIR 57/97 etc.)
- Der sichere Entwicklungs- und Produktlebenszyklus: Cybersecurity/IT-Sicherheit sicherstellen, aufrechterhalten und nach dem Inverkehrbringen überwachen
- Identifikation und Bewertung von Risiken und Bedrohungen (Security-Risikoanalyse, Risikomanagement nach ISO 14971)
- Anforderungen an den Datenschutz von Patientendaten (DSGVO; HIPAA etc.)

Wichtige Hinweise

- Die Inhalte des Seminars berücksichtigen den aktuellen Stand der Regularien / Harmonisierung.
- Das Seminar ist anerkannt als Rezertifizierungsveranstaltung für Absolventen des Lehrgangs „Expert Medical Software (TÜV)“ und wird mit 8 UE angerechnet.
- Als Teilnehmer dieses Seminars erhalten Sie den Bonus eines achtwöchigen kostenfreien Vollzugriffs auf die Online-Produkte „Der CE-Routenplaner“ und "Praxis Medizinprodukterecht" von TÜV Media.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/09540 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto

- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.