



Technischer Datenschutz in Kliniken und Krankenhäusern

30.01.2023
online

Datenschutz- und Informationssicherheitsstandards praktisch umsetzen

[jetzt anmelden](#)

Ihr Referent



Heiko Behrendt

ISO 27001 Auditor
Datenschutz- und IT-Sicherheitsexperte
einer Landes-Prüfbehörde

In kaum einem anderen Bereich ist der Umgang mit personenbezogenen Daten und der damit verbundene Schutz von Betroffenenrechten derart sensibel wie in der Medizin und Pflege. Ein rechtssicheres und technisch lückenloses Datenschutzmanagement in Krankenhäusern und Kliniken erfordert die gezielte Betrachtung der Datenverarbeitungsprozesse bis hin zur Erstellung eines durchgängigen Datenschutzkonzepts, das sowohl Rollen- und Berechtigungskonzepte als auch medizinisch-technische Systeme umfasst. Nach dem neuen § 75c SGB V sind ab dem 1. Januar 2022 alle Krankenhäuser in Deutschland verpflichtet, angemessene organisatorische und technische Vorkehrungen zur IT-Sicherheit zu treffen.

In diesem eintägigen Praxisseminar werden wichtige Aspekte vom Aufbau bis zur Umsetzung eines umfassenden Datenschutzmanagements in Krankenhäusern und Kliniken systematisch aufgezeigt. Ein Schwerpunkt liegt auf der praktischen Umsetzung anerkannter Standards für den Datenschutz und der Informationssicherheit. Dabei werden Inhalte und Zusammenhänge des IT-Grundsicherheitsstandards, der ISO 27001 native, des Branchenspezifischen Sicherheitsstandards für die medizinische Versorgung (B3S) und der Orientierungshilfe Krankenhausinformationssysteme (OH-KIS) ausführlich erklärt. Anschließend werden anhand praktischer Fälle Maßnahmen für die Beseitigung kritischer Schwachstellen in Krankenhäusern und Kliniken dargestellt.

Inhaltsübersicht:

- Datenverarbeitungsprozesse im Krankenhaus bzw. in Kliniken
- Abgrenzung der Verantwortlichkeiten und Zuständigkeiten
- Ausgestaltung des Datenschutz- und Informationssicherheitsmanagements
- Anforderungen des IT-Grundsicherheitsstandards und der ISO 27001 native
- Inhalte des Branchenspezifischen Sicherheitsstandards für die medizinische Versorgung (B3S)
- Anwendung der Orientierungshilfe Krankenhausinformationssysteme (OH-KIS)
- Leitlinie, Schutzziele, Risikomanagement
- Abgrenzung des Informationsverbunds (Scope)
- Toolbasierter Einsatz für die Bearbeitung der Anforderungen für Datenschutz und Informationssicherheit
- Kritische Schwachstellen im Krankenhaus bzw. in Kliniken erkennen und durch Umsetzung von TOMs beseitigen
 - Rollen und Berechtigungskonzept auf der System- und Anwendungsebene
 - Benutzer- und Gruppenkontenverwaltung im Active Directory und in Fachanwendungen des KIS
 - Protokollierung und Zugriffskontrolle
 - Auftragsverarbeitung und Fernwartung
 - Löschkonzept zur Löschung von Patienten- und Falldaten



08:30

Login

09:00

Begrüßung und Vorstellungsrunde

- Vorstellung des Referenten und der TeilnehmerInnen

09:15

Datenschutz und Informationssicherheit im Krankenhaus bzw. in Kliniken

- Abgrenzung der Verantwortlichkeiten und Zuständigkeiten
- Ausgestaltung des Datenschutzmanagements im Krankenhaus-/Klinikbetrieb
- Aufgaben des/der Datenschutz- und Informationssicherheitsbeauftragten
- Zusammenarbeit zwischen „Datenverantwortlichen“, Fachbereichen und dem IT-Management

10:15

Kaffeepause

10:45

Anwendung von anerkannten Sicherheitsstandards für Datenschutz und Informationssicherheit – IT-Grundschutz, ISO 27001 native, Branchenspezifischer Sicherheitsstandard für die medizinische Versorgung (B3S) und Orientierungshilfe Krankenhausinformationssysteme (OH-KIS)

- IT-Grundschutz und ISO 27001 native
- Branchenspezifischer Sicherheitsstandard für die medizinische Versorgung (B3S)
- Orientierungshilfe Krankenhausinformationssysteme (OH-KIS)
- Anforderungen an Betreiber Kritischer Infrastrukturen
- Empfehlungen für die Festlegung der Anwendung der Standards für Datenschutz und Informationssicherheit im Krankenhaus bzw. Kliniken
- Methodische Schritte zur praktischen Umsetzung der festgelegten Strategie

12:30

Mittagessen



13:30

Anforderungen und Umsetzung der Standards für Datenschutz und Informationssicherheit

- Leitlinie zum Datenschutz und zur Informationssicherheit
- Abgrenzung des Informationsverbunds, Scope
- Schutzziele, Schutzbedarfsfeststellung, Risikoanalyse
- Umsetzung der Anforderungen des Standards B3S und der OH-KIS
- Toolbasierter Einsatz für die Bearbeitung der Anforderungen für Datenschutz und Informationssicherheit

14:30

Kaffeepause

15:00

Kritische Schwachstellen im Krankenhaus bzw. in Kliniken erkennen und durch Umsetzung von technischen und organisatorischen Maßnahmen (TOMs) beseitigen

- Rollen und Berechtigungskonzept auf der System- und Anwendungsebene
- Benutzer- und Gruppenkontenverwaltung im Active Directory und in Fachanwendungen
- Protokollierung und Zugriffskontrolle
- Auftragsverarbeitung und Fernwartung
- Löschkonzept zur Löschung von Patienten- und Falldaten

16:30

Ende des Seminars



Heiko Behrendt

Als zertifizierter ISO 27001 Auditor für Informationssicherheit begleitet Heiko Behrendt Behörden und Firmen bei der Einführung und Sicherstellung von IT-Grundschutz- und Datenschutzstandards. Darüber hinaus führt er in seiner Funktion als Datenschutz- und IT-Sicherheitsexperte einer Aufsichtsbehörde Datenschutz-Audits sowie datenschutzrechtliche und sicherheitstechnische Kontrollen der Einhaltung der Datenschutzgrundverordnung durch.

Das sagen unsere Kunden über Datenschutz-Seminare von Heiko Behrendt:

„Sehr umfangreich und anschaulich vorgetragen. Auf Fragen wurde entsprechend eingegangen. Bei der Online-Konferenz gab es keinerlei Probleme.“ (Dirk Grüttner, Landkreis Stade - Personalrat)

„Die Veranstaltung ist sehr informativ und das Vorstellen der Herangehensweise und möglicher Tools ist hilfreich für die Übertragung in die eigene Praxis.“ (Sabrina Fuhrmann, Universität Hamburg)

„komplett super, sehr informativ und hilfreich“ (n.n.)

"Sehr gut verständlich, praxisnah- und sehr gut strukturierter, geduldiger Referent." (n.n.)

"Das Seminar war sehr informativ und sehr gut aufbereitet. Entspricht meinen Erwartungen voll und ganz." (n.n.)

"Technisch hat alles gut funktioniert. Obwohl das Seminar sehr inhaltsreich war, habe ich mich zu keinem Zeitpunkt überfordert gefühlt, weil Herr Behrendt die einzelnen Punkte gut verständlich erläutert hat. Die vermittelten Inhalte werden mir bei meiner täglichen Arbeit weiterhelfen." (n.n.)

Zielgruppe – An wen richtet sich dieses Seminar?

Das Intensiv-Praxisseminar richtet sich nicht nur an Datenschutz- und Informationssicherheitsbeauftragte, sondern auch an Führungskräfte, MitarbeiterInnen und SachbearbeiterInnen, die an technischen und rechtlichen Aspekten des Datenschutzes interessiert sind.



Termin:

30.01.2023

VERANSTALTUNGSORT:

online

TEILNAHMEGEBÜHR:

Online-Teilnahme: 535,- Euro zzgl. MwSt.

Details zur Anmeldung unter:

www.fortbildungskampagne.de/anmeldung

DIE TEILNAHMEGEBÜHR BEINHALTET:

- Schulungsunterlagen (digital)
- Teilnahmezertifikat

Wenn Sie zwei oder mehrere Datenschutz-Seminare buchen, erhalten Sie einen Rabatt von 15%. Die Seminare ergänzen sich inhaltlich.

- 23.01.23 (H.8) Technisches Basiswissen für Personal- und Betriebsräte sowie Personalwesen - Beschäftigtendaten schützen! Überwachung und Einhaltung der DSGVO
- 30.01.23 (H.4) Technischer Datenschutz in Kliniken und Krankenhäusern - Datenschutz- und Informationssicherheitsstandards praktisch umsetzen
- 23.02.23 (H.7) Technisches Basiswissen für Datenschutz- und Informationssicherheitsbeauftragte - Funktionen von Hard- und Software, Gefährdungen sowie technische und organisatorische Maßnahmen einfach erklärt
- 23.03.23 (H.9) DSGVO richtig anwenden (Recht) - Wichtige Regelungen der DSGVO praktisch umsetzen
- 24.04.23 (H.1) Datenschutzaudits und Datenschutzkontrolle mit Methode - Überwachung der Einhaltung der DSGVO durch den/die Datenschutzbeauftragte(n)
- 11.05.23 (H.10) Auftragsverarbeitung in Rechenzentren - Housing, Hosting und Cloud-Dienste sicher gestalten
- 25.05.23 (H.3) Datenschutz und Informationssicherheit auf der Basis von IT-Grundschutz
- 13.06.23 (H.5) Datenschutz für mobile IT-Systeme, im Homeoffice und für Bring Your Own Device - Schwachstellendurch technische und organisatorische Maßnahmen beseitigen

ANMELDUNG:

Bitte verwenden Sie zur Anmeldung unser Online-Anmeldeformular unter: www.fortbildungskampagne.de/anmeldung

KONTAKT FÜR RESERVIERUNGEN UND BUCHUNGEN:

Haben Sie Fragen zum Seminar oder zu Reservierungen und Buchungen?

Schreiben Sie uns einfach eine Email oder rufen Sie uns unter der folgenden Rufnummer an:

Email: team@fortbildungskampagne.de | Telefon: +49 (0) 30 89 56 27 16

TEILNAHME- UND STORNIERUNGSKONDITION (AUSZUG):

Die verbindliche Anmeldung erfolgt über unser Online-Anmeldeformular und wird durch Zusendung einer Anmeldebestätigung sowie der Rechnung bestätigt. Stornierungen sind bis vier Wochen vor Veranstaltungsbeginn kostenfrei, bereits gezahlte Beträge werden erstattet. Bei kurzfristiger Stornierung oder beispielsweise krankheitsbedingter Abwesenheit ist die Benennung eines Ersatzteilnehmers jederzeit möglich. Sofern sich kein Ersatzteilnehmer findet, kann nach Absprache ein Gutschein ausgestellt werden, der zur Teilnahme an einem Nachfolgetermin oder einem ähnlichen Seminar berechtigt. Bitte beachten Sie unsere AGB, die unter dem folgenden Link aufgerufen werden können:

DATENSCHUTZHINWEISE:

Wir weisen darauf hin, dass Sie die Verwendung Ihrer Daten gemäß unserer Datenschutzbestimmungen durch eine Nachricht an datenschutz@fortbildungskampagne.de selbstverständlich jederzeit widerrufen können. Bitte beachten Sie unsere Datenschutzbestimmungen, die unter dem folgenden Link aufgerufen werden können:

HINWEISE ZUM DATENSCHUTZ BEI ONLINE-TEILNAHME:

Details zur technischen Umsetzung der Online-Teilnahme erhalten Sie im Anschluss an Ihre Anmeldung. Ein wirksamer Auftragsverarbeitungsvertrag mit dem technischen Dienstleister liegt vor. Durch die Fortbildungskampagne als Veranstalter erfolgt während der Online-Teilnahme keine Speicherung von schriftlichen, akustischen oder visuellen Daten der Teilnehmenden. Eine temporäre Protokollierung des Chat-Verlaufes einer Online-Veranstaltung wird binnen zwei Arbeitstagen nach der Veranstaltung gelöscht. Bitte beachten Sie, dass Sie im Rahmen Ihrer Online-Teilnahme möglicherweise unfreiwillig Daten und Informationen übertragen, etwa durch weitere Personen in Ihrem Raum. Eine mögliche Übertragung derartiger Informationen liegt in Ihrem Verantwortungsbereich.