ISO 27001 (nicht nur) für Medizinproduktehersteller

Mit Dr. Andre Baumgart, Prof. Dr. Christian Johner

Transkript

00:00:05 Sprecher 1

Medical Device Insights, ein Podcast des Jona Instituts für Medizinproduktehersteller, Behörden und benannte Stellen.

00:00:17 Sprecher 2

Spätestens mit der DiGA-Verordnung ist die ISO 27001 und Informationsmanagementsysteme im Allgemeinen sind im Fokus

00:00:28 Sprecher 2

einiger Medizinproduktehersteller geraten.

00:00:31 Sprecher 2

Allerdings sollten nicht nur diese DiGA-Hersteller sich mit dieser Norm auseinandersetzen und um was es in dieser Norm geht, was sie da genau fordert, wie man das einführt, so ein Informationssicherheitsmanagementsystem.

00:00:46 Sprecher 2

Genau darüber möchte ich heute sprechen mit meinem Kollegen, dem Doktor Andre Baumgart.

00:00:51 Sprecher 2

Hallo Andre, wie geht es dir?

00:00:53 Sprecher 2

Möchtest du dich ganz kurz vorstellen?

00:00:55 Sprecher 3

Vielen Dank, Christian, für die Einführung.

00:00:56 Sprecher 3

Mein Name ist André Baumgardt.

00:00:58 Sprecher 3

Ich beschäftige mich am UNI Institut mit der Medizinproduktezulassung und dem Informationssicherheitsmanagement, insbesondere im Kontext von DiGAs und bin selbst Lead Auditor im Bereich 27001

und Lead Auditor im Bereich ISO 13485 und hab schon ja mittlerweile mehrere 100 Hersteller unterstützt bei der Zulassung von Medizinprodukten.

00:01:23 Sprecher 2

Damit bist du natürlich genau der richtige Mann, wenn es um dieses Thema geht.

00:01:27 Sprecher 2

Starten wir mit den Anfängen oder mit den Grundlagen.

00:01:30 Sprecher 2

Was ist denn so ein Informationssicherheitsmanagementsystem?

00:01:35 Sprecher 2

Was regelt das und wie unterscheidet sich das von einem Qualitätsmanagementsystem?

00:01:42 Sprecher 3

Ein Informationssicherheitsmanagementsystem befasst sich, wie der Name schon sagt, um das Thema Sicherheit mit Informationen und Daten in der Organisation

00:01:51 Sprecher 3

Und im Prinzip ist es ‚n systematischer, risikobasierter und zielgerichteter Ansatz, um das Management von Informationen in der Organisation zu gestalten und damit die Geschäftsziele des Unternehmens zu unterstützen und zu erreichen.

00:02:10 Sprecher 2

Was fordert jetzt so ‚ne ISO 27001 konkret?

00:02:15 Sprecher 2

geht von den Herstellern, muss man da auch Verfahrensanweisungen implementieren, wie bei einer 13485?

00:02:24 Sprecher 3

Die Norm schreibt einige Prozesse vor, im Vergleich zu ISO 13485 deutlich weniger,

00:02:35 Sprecher 3

was meistens Hersteller damit überrascht, aber es handelt sich dabei um teilweise ähnliche Themen wie die 13485, die auch Anknüpfungspunkte liefern.

00:02:46 Sprecher 3

Themen wie Beschreibung des Anwendungsbereichs, des Kontext der Organisation kennen wir auch aus der ISO 13485 Das ganze Thema Führung, Führungsverantwortung, Verpflichtung der Unternehmensleitung spielt ja auch ‚ne Rolle.

00:03:04 Sprecher 3

Dann ein risikobasierter Ansatz jetzt bezüglich der Werte und Informationen, das kennen wir aus der ISO 13485 bezüglich der Risiken zu Medizinprodukten.

00:03:16 Sprecher 3

Also ist es hier etwas anders gelagert, aber vom Ansatz her ähnlich.

00:03:21 Sprecher 3

Und das ganze Thema Unterstützung, Ressourcen in der Organisation, das ist auch etwas, was sehr ähnlich ist im Vergleich zur 13485.

00:03:32 Sprecher 3

dann wir haben hier auch ‚ne Managementbewertung, interne Audits und den beliebten Kappa-Prozess, der auch hier wirkt.

00:03:41 Sprecher 3

Also man sieht schon oder hört daraus, dass es viele Anknüpfungspunkte in den Hauptartikeln der Norm gibt.

00:03:50 Sprecher 2

Jetzt hast du gerade geschildert, dass wir viele ähnliche Verfahrenprozesse haben.

00:03:55 Sprecher 2

Du sprachst jetzt von Management-Reviews, von den Korrektivmaßnahmen, Vorbeugemaßnahmen von internen Audits.

00:04:01 Sprecher 2

Wo siehst du die größten Unterschiede?

00:04:04 Sprecher 2

Also, welche Prozesse müssten Unternehmen zusätzlich implementieren, um auch den Anforderungen nach 27001 gerecht zu werden?

00:04:14 Sprecher 3

Die Unterschiede liegen, weil der Fokus der Norm ja ein anderer ist im Bereich Sicherheit und Information und Schutz der Werte in der Organisation, insbesondere eben im Anhang A1.

00:04:30 Sprecher 3

dort werden viele Anforderungen genannt, die einen anderen Aspekt der Organisation beleuchten, wie die ISO 13485.

00:04:42 Sprecher 3

Also, Beispiele kann man nehmen.

00:04:44 Sprecher 3

Es gibt eine Richtlinie für die Informationssicherheit, die man implementieren muss, um festzulegen, auf was sich diese Informationssicherheitsmanagementsysteme beziehen.

00:04:58 Sprecher 3

Und alles Weitere wird dann abgeleitet im Bereich zum Beispiel mobile Geräte, Telearbeit, Personalsi-

cherheit, Zugangsberechtigungen, Verwaltung der Informationswerte, Schutz von Datenträgern, Gebäuden.

00:05:14 Sprecher 3

Das sind alles Verantwortlichkeiten, die man hier festlegen muss und dort braucht es im Spezifischen dann Verfahrensanweisungen, aber dann auch wahrscheinlich

00:05:26 Sprecher 3

Arbeitsanweisungen im Detail, um den Mitarbeitenden Werkzeuge an die Hand zu geben und auch Anleitungen zu geben, wie sie das umsetzen sollen.

00:05:35 Sprecher 2

Jetzt hast du ganz viel über die ISO 27001 gesprochen.

00:05:40 Sprecher 2

Jetzt gibt es in dieser Serie noch ein paar Schwesternormen, speziell auch eine für die Gesundheitsanwendung oder fürs Gesundheitswesen.

00:05:50 Sprecher 2

Würdest du Herstellern empfehlen,

00:05:52 Sprecher 2

diese anderen Normen auch zu betrachten und vielleicht noch ‚ne Frage davor, um was geht es in diesen Schwesternormen?

00:06:00 Sprecher 3

Es gibt ‚ne ganze Normenfamilie der 27 Tausender Reihe.

00:06:05 Sprecher 3

Die Kernnorm, die 27001, über die wir jetzt bisher primär gesprochen haben, beschreiben die Anforderungen des I.S.M.S.

00:06:16 Sprecher 3

für allgemeine Organisationen.

00:06:19 Sprecher 3

Jetzt, wenn man, wie du angesprochen hast, die 27 799 betrachtet, die speziell für Gesundheitsversorgungseinrichtungen auch entworfen wurde, die befasst sich eben mit den Spezifika, die in Versorgungseinrichtungen oder eben bei Betreibern, wenn man verallgemeinert spricht, vorliegen und verschärft teilweise die Anforderungen in

00:06:46 Sprecher 3

wirklich konkrete Vorgaben, die erfüllt sein müssen bezüglich der Umsetzung dieser Informationssicherheitsanforderungen.

00:06:56 Sprecher 2

Könntest du uns ein Beispiel vergeben für diese Verschärfungen?

00:06:59 Sprecher 3

Ein Beispiel ist, dass die Leitlinie zur Informationssicherheit einen konkreten Hinweis und konkrete Ausgestaltung der persönlichen Gesundheitsinformationen beinhalten muss.

00:07:14 Sprecher 3

Das bedeutet also, dass diese Leitlinie schon auf oberster Ebene definiert, wie ich mit diesen sensiblen Informationen und Daten in der Organisation umgehe.

00:07:24 Sprecher 3

Auf den verschiedenen Ebenen, in den verschiedenen Bereichen, zum Beispiel eines Krankenhauses oder auch, wenn ich ein DIGA-Hersteller bin, wie gehen Entwickler mit potenziellen Daten an, die vielleicht eine KI trainieren und wie geht der Customer Service mit diesen Kundendaten um?

00:07:40 Sprecher 3

Das muss ich

00:07:41 Sprecher 3

eben explizit festlegen, schon auf oberste Ebene in meinem Informationssicherheitsmanagementsystem.

00:07:50 Sprecher 2

Damit hast du jetzt ,n weiteren spannenden Gedanken hier mit reingebracht gehabt, nämlich das Thema Produkte.

00:07:56 Sprecher 2

Viel haben wir gesprochen, jetzt eben über Organisationen, die ihre Informationen, Informationstechnik schützen muss.

00:08:03 Sprecher 2

Das würde wahrscheinlich vor allem die Betreiber betreffen.

00:08:07 Sprecher 2

Jetzt sind aber viele DiGA-Hersteller ja nicht nur Betreiber, sondern vor allem auch Hersteller von Medizinprodukten.

00:08:13 Sprecher 2

Und die MDR stellt an diese Medizinprodukte ja auch explizit die Anforderung, die Informationssicherheit nach State of the Art berücksichtigen zu müssen.

00:08:25 Sprecher 2

Ist uns die ISO 27001 hilfreich dabei, diese Anforderung der MDR zu erfüllen?

00:08:34 Sprecher 3

ISO 27001 als Systemnorm kann indirekt dabei helfen, Anforderungen abzuleiten für die Produkte, weil ich natürlich, wenn ich später an den Betrieb und auch die Produktrealisierung denke, nachprüfe

00:08:55 Sprecher 3

muss, ob ich nachher in meinem Anwendungskontext sicher betrieben werden kann.

00:09:00 Sprecher 3

Also, es ist eher ‚n indirekter Bezug, wenn man den direkten Bezug will, dann hilft einem die Norm durch den systematischen Ansatz in der Organisation als Hersteller, diese Anforderungen systematisch abzuleiten.

00:09:16 Sprecher 3

Also, ob das kryptographische Verfahren sind oder das Thema Authentifizierung für

00:09:23 Sprecher 3

für so eine App, da kann ich dann systematisch Anforderungen ableiten, die aber heute häufig verlinken auf spezifischere Produktnormen oder Anforderungen, wie beispielsweise vom Bundesinstitut für Sicherheit in der Informationstechnik, die ja zumindest in einer Draft-Version Anforderungen an digitale Produkte beispielsweise herausgegeben hat.

00:09:50 Sprecher 3

Oder natürlich haben wir auch unseren Leitfaden, den

00:09:53 Sprecher 3

der uns sehr gut unterstützt in der Beratung, aber vor allem auch die Hersteller unterstützt bei der Ableitung von Anforderungen für die Produkte.

00:10:03 Sprecher 2

Ich fass ganz kurz noch mal zusammen, damit du prüfen kannst, ob ich es richtig verstanden hab.

00:10:08 Sprecher 2

Ich hab dich so verstanden, dass die ISO 27001 letztlich auch genutzt werden kann, um die Produktanforderung, also die System Requirements Specification oder Software Requirement Specification, zu

00:10:21 Sprecher 2

zu erstellen, damit man so nachher aus Kundensicht da auch Produkte hat, die gemäß 27001 betrieben werden können, dass wir aber als Hersteller explizit eben auch andere Normen und Best Practices ranziehen müssen.

00:10:39 Sprecher 2

und für diejenigen, für die das zu viel Arbeit ist, sich da viele Normen, wie zum Beispiel jetzt ‚ne IEC 62 443 noch mal reinziehen zu müssen, für die empfiehlst du dann unseren Leitfaden, in dem wir das alles schon konsolidiert haben.

00:10:51 Sprecher 2

Stimmt das so?

00:10:52 Sprecher 3

Das stimmt so und unterstützt sich und das bringt natürlich ‚ne Menge Effizienz, wenn man sich auf die bestehenden Dokumentationen bezieht.

00:11:01 Sprecher 2

Lass uns noch mal zurückgehen zum Thema Informationssicherheitsmanagementsysteme.

00:11:07 Sprecher 2

und zur Frage, wie geht man jetzt vor, um sowas einzuführen.

00:11:12 Sprecher 2

Die meisten Hersteller beginnen ja da nicht bei 0, die müssen ja laut M.D.R.

00:11:16 Sprecher 2

über ein Qualitätsmanagementsystem bereits verfügen.

00:11:20 Sprecher 2

Welche Schritte empfiehlst du jetzt, um zu den Anforderungen der ISO 27001 zusätzlich zu genügen?

00:11:29 Sprecher 2

Da steckt auch ein bisschen die Frage mit drin, haben wir nachher 2 Managementsysteme und

00:11:35 Sprecher 2

Auch die andere Frage steckt da mit drin.

00:11:38 Sprecher 2

Also, welche Schritte gehe ich jetzt, um von einem Q.

00:11:41 Sprecher 2

M.

00:11:41 Sprecher 2

System zur 27001 Konformität zu kommen.

00:11:48 Sprecher 3

Zunächst muss ich die Organisation fragen, was will ich mit diesem Informationssicherheitsmanagementsystem als Hersteller

00:11:58 Sprecher 3

Und das ist im Prinzip eine strategische Frage und die Anforderung, so etwas zu haben, kommt in der Regel entweder klassischerweise aus der Regulierung, gesetzliche Vorgaben, wie wir es jetzt im Bereich der DiGAs haben, oder häufig eben auch von Kunden.

00:12:15 Sprecher 3

Also das Erste, was man machen muss, ist sich zu fragen, lohnt es sich, das Ganze durchzuführen, muss ich das sogar machen, um überhaupt am Markt bestehen zu können?

00:12:25 Sprecher 3

Das wäre der erste Schritt.

00:12:27 Sprecher 3

der zweite Schritt, wenn ich mich dann dafür entschieden habe, machen wir klassischerweise eine detaillierte Gap-Analyse, wo wir alle Anforderungen der Hauptkapitel und des Anhang A.

00:12:40 Sprecher 3

1 durchgehen und festhalten, was liegt denn in der Organisation vor.

00:12:46 Sprecher 3

Somit können wir auch feststellen, wie gut schon bestehende Verfahrensanweisungen die Anforderungen der ISO 27001 abdecken.

00:12:56 Sprecher 3

Und

00:12:57 Sprecher 3

gleichzeitig kriegen wir dann auch ‚n gutes Bild, wie viel Aufwand dahinter steckt, das ganze System umzusetzen, also im ganz konkret im im Falle von Manntagen oder dann eben auch Kosten, die man da hinten dran legt.

00:13:11 Sprecher 3

Und darauf basierend kommt der dritte Schritt, die Umsetzungsplanung und die Umsetzungsplanung ist dann eben ein multidisziplinäres Unterfangen in der Organisation, um alle

00:13:24 Sprecher 3

nicht nur die Entwickler oder nicht nur die I.

00:13:26 Sprecher 3

T.

00:13:27 Sprecher 3

Abteilung, sondern wirklich alle mitzunehmen, um das Thema Informationssicherheit zu leben.

00:13:32 Sprecher 3

Weil letztlich geht es eben nicht nur um I.

00:13:35 Sprecher 3

T.

00:13:35 Sprecher 3

Fragen bei diesem Thema, sondern auch um real physische Elemente, die hier in der Organisation zur Informationssicherheit beitragen.

00:13:44 Sprecher 3

Und das muss ich dann klassischerweise eben aufbauen, umsetzen, leben und zu einem gewissen Grad kommt an der

00:13:53 Sprecher 3

vierte Schritt, dass man das intern auditiert, dieses interne Audit dazu nutzt, um noch Lücken festzustel-

len in der Umsetzung und das Ganze dann zur Vorlage bringt in einer Managementbewertung.

00:14:06 Sprecher 3

Und wenn man das mal durchlaufen hat, dann kann man eben davon sprechen, dass man es, denke ich, einmal überprüft hat, wie das Ganze gelebt werden soll.

00:14:16 Sprecher 3

Und wenn ich sicher bin, dass ich somit alle oder wesentliche Anforderungen in der Norm und im Anhang A.

00:14:23 Sprecher 3

1 erfülle und die auch richtig umgesetzt habe, dann melde ich mich zum Audit an von einer unabhängigen Prüfstelle, die dann ein ISO 27001 Zertifikat nach erfolgreicher Prüfung ausstellen wird.

00:14:39 Sprecher 2

Du hast jetzt schon einen Satz oder ein Wort genannt, das mich aufhören ließ.

00:14:43 Sprecher 2

Es war nämlich jetzt der

00:14:44 Sprecher 2

Aufwand.

00:14:45 Sprecher 2

Ich glaube, viele der Hersteller interessieren sich dafür, was bedeutet es jetzt zeitlich, was bedeutet es auch kostenmäßig, was sind da deine Erfahrungen, mit wie viel Aufwand muss man als Hersteller rechnen, um 27001 zertifizierungsbereit zu sein?

00:15:02 Sprecher 3

Den Aufwand, den wir jetzt in der Vielzahl von Projekten gesehen haben, schwankt zwischen 60 und 100 Manntagen, kann man grob sagen.

00:15:09 Sprecher 3

Also, wenn man jetzt mal die Mitte nimmt von 80 Manntagen, dann kann man das als Aufwand für die Organisation, die Unternehmung rechnen.

00:15:17 Sprecher 3

Das sind interne Manntage oder Frau-Tage, die man entsprechend braucht, um das Ganze aufzubauen, zu betreiben und in der Organisation inklusive Schulungen umzusetzen.

00:15:31 Sprecher 2

Ja, ich glaube, damit haben wir eine ganz gute Übersicht.

00:15:34 Sprecher 2

Lass mich kurz zusammenfassen.

00:15:35 Sprecher 2

Wir haben also einmal drüber gesprochen, was so ein Informationsmanagementsystem überhaupt alles regelt.

00:15:41 Sprecher 2

Haben erkannt, dass es viele Verfahrensanweisungen gibt, die wir aus einer ISO 13485 bereits kennen, dass aber weitere Arbeits und Verfahrensanweisungen notwendig sind, um speziell die Anforderung dieses Anhangs

00:15:56 Sprecher 2

A.

00:15:57 Sprecher 2

1 abzudecken, wo es dann eben um ganz konkrete Dinge auch geht, wie Zugangsberechtigungen hast du geschildert gehabt, auch Personal einstellen, Zugang zu Systemen und vieles Weiteres mehr.

00:16:08 Sprecher 2

Wir hatten einen kurzen Blick geworfen in die Normen Familie.

00:16:12 Sprecher 2

Du hast berichtet, dass es für Betreiber von Gesundheitseinrichtungen noch mal eine weitere Norm gibt, nämlich die ISO 27 799 in dieser Familie der 27 Tausender Serie.

00:16:24 Sprecher 2

Wir haben

00:16:25 Sprecher 2

drüber gesprochen gehabt, dass die M.D.R.

00:16:28 Sprecher 2

die Informationssicherheit fordert, dass eine 27001 jetzt aber nicht ausreichen wird, sondern eher eigentlich Hinweise zur Spezifikation von diesen Produkten gibt und dass man dann andere produktspezifische Normen noch braucht.

00:16:42 Sprecher 2

Und am Schluss hast du berichtet, dass wir schon mit 4 Schritten letztlich zur Zertifizierung kommen können und was das an Aufwand bedeutet.

00:16:50 Sprecher 2

Oh, ich denke, es war eine ganze Menge in dieser guten Viertelstunde,

00:16:54 Sprecher 2

André, vielen Dank, dass du für uns da warst, uns diesen Einblick gewährt hast.

00:16:59 Sprecher 2

Ja, und für alle, die noch mehr wissen wollen zu diesem Thema, wir haben Ihnen Fachartikel hier unten in der Beschreibung wieder verlinkt.

00:17:07 Sprecher 2

Unsere Kontaktdaten kennen Sie ja eh.

00:17:09 Sprecher 2

Also, wenn wir helfen können bei der Einführung oder bei der Prüfung der Zertifizierungsreadiness sozusagen, da geben Sie einfach Bescheid, damit

00:17:20 Sprecher 2

Ihr System eben den Anforderungen beispielsweise nach DiGA-Verordnung genügt bzw.

00:17:25 Sprecher 2

Ihre Produkte auch MDR-konform sind.

00:17:28 Sprecher 2

André, danke, dass du wieder dabei warst.

00:17:31 Sprecher 3

Ganz herzlichen Dank.

00:17:32 Sprecher 2

Bis bald.

00:17:32 Sprecher 2

Tschüss.

00:17:34 Sprecher 3

Tschüss.