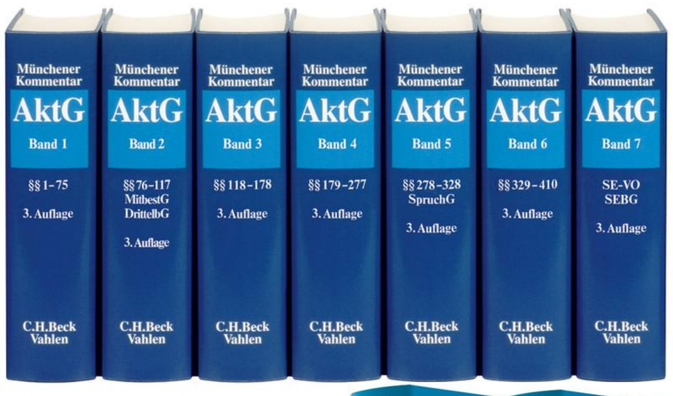
Risikomanagement als Aufgabe der Kliniksleitung

Gesellschaft für klinische Dienstleistungen Düsseldorf mbH
Ein Tochterunternehmen des Universitätsklinikums Düsseldorf

B. Schütze[1)], S. Walther[2)]

1) GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH, Düsseldorf
2) Universitätsklinikum Düsseldorf, Dezernat für Informations- und Kommunikationstechnologie, Düsseldorf

Einleitung: Das Erkennen und Steuern von Risiken, die sich im Zusammenhang mit dem Produktionsfaktor Information ergeben, der so genannte Risikomanagementprozess, ist eine Aufgabe, welche für eine Klinik lebensnotwenig ist. Einige rechtliche Grundlagen werden hier vorgestellt, wobei - bedingt durch die Privatisierung diverser Krankenhäuser - auch ein Blick außerhalb des öffentlichen Bereiches geworfen wird.



Das **Aktiengesetz** (AktG) fordert von Unternehmen, Risikofrüherkennungssysteme, Risikomanagement- und -steuerungssysteme zu installieren sowie potenzielle Risikofelder zu beobachten und den davon ausgehenden Risiken gegenzusteuern:

> §91
> ...
> (2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Ergänzend hierzu das HBG:

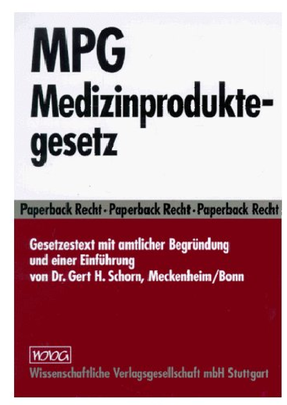
> § 317 Gegenstand und Umfang der Prüfung
> ...
> (4) (4) Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.

Durch das **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich** (KonTraG) wurde die Pflicht der Vorstände börsennotierter Aktiengesellschaften, ein Risikomanagement zu installieren, rechtlich verankert. Die Einrichtung eines Risikomanagementsystems (RMS) ist dabei zunächst nur für Aktiengesellschaften gesetzlich vorgeschrieben. Ausgehend von der Begründung zum KonTraG wird das Gesetz auch Ausstrahlungswirkungen auf andere Gesellschaftsformen haben, so dass je nach Größe, Komplexität und Struktur eines Unternehmens insbesondere die Geschäftsführer von GmbHs von diesen Regelungen betroffen sind. Hinzu kommt, dass Vorstände von Konzernen, Beteiligungsgesellschaften etc. nach den Überlegungen des Gesetzgebers ihrer Verpflichtung zum Risikomanagement konzernweit nachkommen müssen. Da auch von Tochterunternehmen bestandsgefährdende Risiken ausgehen können, spielt deren Rechtsform insoweit keine Rolle.

Krankenhäuser und Arztpraxen, welche ihren Beschäftigten erlauben privat im Internet zu surfen oder eMails abzurufen, gelten laut Gesetz als Telekommunikationsdiensteanbieter; entsprechend gilt die entsprechende Gesetzgebung.
Das **Telekommunikationsgesetz** (TKG) enthält in den §§ 88 bis 115 Regelungen zum Schutz des Fernmeldegeheimnisses, zum Datenschutz und zu Belangen der öffentlichen Sicherheit.
§109 verpflichtet den Diensteanbieter technische Schutzvorkehrungen zum Schutz des Fernmeldegeheimnisses sowie der personenbezogenen Daten zu treffen sowie die entsprechenden Systeme gegen unerlaubte Zugriffe zu sichern.
Dies bedeutet z.B..:

- Spam- und Virenschutz können seitens Personalret (oder wenn nicht vorrhanden: Einzelverträge mit Mitarbeitern) mitbestimmungspflichtig sein; §89 Abhörverbot, §109 Technische Schutzmaßnahmen)
- Der Anbieter muss Vorsorge treffen, dass die Dienstleistung nicht ausfällt §109 Technische Schutzmaßnahmen)

Nach dem **Medizinproduktegesetz** und den europäischen Richtlinie 93/42/EWG für Medizinprodukte ist das Risikomanagement eine zwingende Voraussetzung für Hersteller von Medizinprodukten.



> § 30 Sicherheitsbeauftragter für Medizinprodukte
> (1) Wer als Verantwortlicher nach § 5 Satz 1 und 2 seinen Sitz in Deutschland hat, hat unverzüglich nach Aufnahme der Tätigkeit eine Person mit der zur Ausübung ihrer Tätigkeit erforderlichen Sachkenntnis und der erforderlichen Zuverlässigkeit als Sicherheitsbeauftragten für Medizinprodukte zu bestimmen.
> ...
> (4) Der Sicherheitsbeauftragte für Medizinprodukte hat bekannt gewordene Meldungen über Risiken bei Medizinprodukten zu sammeln, zu bewerten und die notwendigen Maßnahmen zu koordinieren. Er ist für die Erfüllung von Anzeigepflichten verantwortlich, soweit sie Medizinprodukterisiken betreffen.

Empfohlen hierzu, wenn auch nicht gesetzlich vorgeschrieben, ist der Einsatz der **DIN EN ISO 14971,** welche den gesamten Prozess des Risikomanagements abdeckt. Bei der Einbindung von Medizinprodukten in Netzwerke soll die sich derzeit noch im Entwurf befindliche Norm **DIN EN 80001-1** die Anwendung des Risikomanagements beschreiben.

Am Mittwoch,dem 08.09, findet die Gründungssitzung der Projektgruppe “Medizintechnik in der Medizinischen Informatik” statt, die sich mit allen Themengebieten zu diesem Gegenstand beschäftigt:
Zeit 18:15 – 20:15 Uhr
Gebäude 1, 2.OG, Raum 212

Kontakt: schuetze@medizin-informatik.org