

DIN EN ISO 27799

ICS 35.240.80

**Medizinische Informatik –
Sicherheitsmanagement im Gesundheitswesen bei Verwendung der
ISO/IEC 27002 (ISO 27799:2008);
Deutsche Fassung EN ISO 27799:2008**

Health informatics –
Information security management in health using ISO/IEC 27002 (ISO 27799:2008);
German version EN ISO 27799:2008

Informatique de santé –
Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002
(ISO 27799:2008);
Version allemande EN ISO 27799:2008

Gesamtumfang 71 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (EN ISO 27799:2008) wurde von der WG III „Security, Safety and Quality“ des CEN/TC 251 „Medizinische Informatik“ übernommen und im Rahmen eines gemeinsamen Projektes mit dem ISO/TC 215 „Health Informatics“ erarbeitet. Der Fachbereich 7 „Medizinische Informatik“ und insbesondere die Mitarbeiter des NA 063-07-04 AA „Sicherheit“ des Normenausschusses Medizin (NAMed) im DIN haben an der Erarbeitung mitgewirkt.

Für die im Abschnitt 2 zitierten Internationalen Normen wird im folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 27002:2005 siehe DIN ISO/IEC 17799

Zusammenfassung

Diese Norm legt Leitlinien zur Unterstützung von Interpretation und Implementierung der ISO/IEC 27002 (Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Management der Informationssicherheit, früher ISO/IEC 17799) in der Medizinischen Informatik fest und ist eine Ergänzung zur ISO/IEC 27002. Sie legt einen Satz detaillierter Steuerungswerkzeuge zur Handhabung der Informationssicherheit im Gesundheitswesen fest und bietet optimale Leitlinien der Medizinischen Informatik. Nach deren Implementierung können Gesundheitsorganisationen und andere Verwalter von Gesundheitsinformationen ein minimal notwendiges Sicherheitsniveau entsprechend den Erfordernissen ihrer Organisation sicherstellen. Dies dient dann auch der Einhaltung von Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Gesundheitsinformationen.

Gesundheitsinformationen existieren in vielfältiger Form. Sie bestehen aus Daten, die nicht nur in Worten und Zahlen dargestellt werden, sondern auch in Form von Tonaufzeichnungen, Grafiken, Videos und medizinischen Bildern. Gesundheitsinformationen können ausgedruckt oder geschrieben werden, sie können sowohl elektronisch als auch auf Papier aufbewahrt werden. Die Übertragung kann per Hand, mittels Fax, über Computernetzwerke oder per Post erfolgen. Unabhängig von Form und Übertragungsmedium müssen Gesundheitsinformationen immer angemessen geschützt werden.

Die vorliegende Norm und ISO/IEC 27002 legen gemeinsam fest, **was** die geforderten Bedingungen für die Informationssicherheit im Gesundheitswesen sind; sie legen nicht fest, **wie** diese erreicht werden sollen. Deshalb ist der Norm-Entwurf in größtmöglichem Maße technologieunabhängig. Neutralität im Bezug auf die technische Implementierung ist eine wichtige Charakteristik dieser Normen. Die Sicherheitstechnologie befindet sich in einer stetigen schnellen Weiterentwicklung, und die Veränderungen werden zurzeit eher in Monaten als in Jahren gemessen. Im Gegensatz dazu sind Normen, obwohl sie periodisch überprüft werden, insgesamt auf eine Gültigkeit für mehrere Jahre hin angelegt. Genau so wichtig ist es, dass technologische Unabhängigkeit den Herstellern und Dienstleistern die freie Wahl lässt, auch neue oder in Entwicklung befindliche Technologien zu empfehlen, die die in dieser Norm beschriebenen notwendigen Anforderungen erfüllen.

Wie in der Einleitung beschrieben, ist die Kenntnis der ISO/IEC 27002 unabdingbar für das Verständnis dieser Norm.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 17799:2007, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informations-sicherheits-Management (ISO/IEC 17799:2005)*

Deutsche Fassung

**Medizinische Informatik —
Sicherheitsmanagement im Gesundheitswesen bei Verwendung
der ISO/IEC 27002
(ISO 27799:2008)**

Health informatics —
Information security management in health using
ISO/IEC 27002
(ISO 27799:2008)

Informatique de santé —
Gestion de la sécurité de l'information relative à la santé en
utilisant l'ISO/CEI 27002
(ISO 27799:2008)

Diese Europäische Norm wurde vom CEN am 15. Juni 2008 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	7
1.1 Allgemeines	7
1.2 Ausschlüsse aus dem Anwendungsbereich	7
2 Normative Verweisungen	8
3 Begriffe	8
3.1 Begriffe aus dem Gesundheitswesen.....	8
3.2 Begriffe aus dem Bereich der Informationssicherheit.....	9
4 Abkürzungen	11
5 Sicherheit von Gesundheitsinformationen	12
5.4 Zu schützende Gesundheitsinformationen.....	14
5.5 Bedrohungen und Schwachstellen der Sicherheit von Gesundheitsinformationen	14
6 Praktischer Arbeitsplan für die Umsetzung der ISO/IEC 27002	15
6.1 Systematik der Normen ISO/IEC 27002 und ISO/IEC 27001	15
6.2 Engagement des Managements bei der Umsetzung der ISO/IEC 27002.....	16
6.3 Einrichten, betreiben, pflegen und verbessern des ISMS	17
6.4 Planen: Einführen des ISMS	17
6.5 Ausführen: Umsetzen und Betreiben des ISMS	26
6.6 Überprüfen: Überwachen und Überprüfen des ISMS.....	27
6.7 Handeln: Pflegen und Verbessern des ISMS	29
7 Folgerungen aus ISO/IEC 27002 für die Gesundheitsversorgung.....	29
7.1 Allgemeines.....	29
7.2 Leitlinie zur Informationssicherheit	29
7.3 Organisation der Informationssicherheit	31
7.4 Management organisationseigener Werte	34
7.5 Personalsicherheit.....	36
7.6 Physische und umgebungsbezogene Sicherheit.....	39
7.7 Betriebs- und Kommunikationsmanagement	41
7.8 Zugriffskontrolle	46
7.9 Beschaffung, Entwicklung und Wartung von Informationssystemen	50
7.10 Umgang mit Informationssicherheitsvorfällen	52
7.11 Informationssicherheitsaspekte beim Management zur Aufrechterhaltung des Geschäftsbetriebs.....	53
7.12 Einhaltung von Vorgaben	54
Anhang A (informativ) Bedrohungen der Sicherheit von Gesundheitsinformationen.....	56
Anhang B (informativ) Aufgaben und zugehörige Dokumente des Informationssicherheits- Managementsystems	61
Anhang C (informativ) Mögliche wirtschaftliche Vorteile und erforderliche Eigenschaften von Unterstützungs-Tools	65
Literaturhinweise	68

Vorwort

Dieses Dokument (EN ISO 27799:2008) wurde vom Technischen Komitee ISO/TC 215 „Health Informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2009, und etwaige entgegenstehende nationale Normen müssen bis Januar 2009 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 27799:2008 wurde vom CEN als EN ISO 27799:2008 ohne irgendeine Abänderung genehmigt.

Einleitung

Diese internationale Norm ist eine Anleitung für Organisationen der Gesundheitsversorgung und andere Verwahrer persönlicher Gesundheitsinformationen, wie Vertraulichkeit, Integrität und Verfügbarkeit solcher Informationen durch die Umsetzung von ISO/IEC 27002¹⁾ am besten zu schützen sind. Speziell die vorliegende internationale Norm behandelt die spezifischen Belange des Informationssicherheitsmanagements im Gesundheitssektor und seines ganz speziellen Arbeitsumfelds. Obwohl der Schutz und die Sicherheit persönlicher Informationen für jeden einzelnen, jede Organisation, jede Einrichtung und Behörde von Bedeutung sind, gibt es im Gesundheitssektor spezielle Anforderungen, die erfüllt werden müssen, um Vertraulichkeit, Integrität, Auditierbarkeit und Verfügbarkeit persönlicher Gesundheitsinformationen sicherzustellen. Diese Art von Informationen wird häufig als eine der am besten zu schützenden aller Arten von persönlicher Informationen angesehen. Der Schutz der Vertraulichkeit ist grundlegend, falls die Privatsphäre der behandelten Personen zu wahren ist. Die Integrität von Gesundheitsinformationen muss sichergestellt werden, um die Patientensicherheit zu schützen, und eine wichtige Komponente dieser Schutzmaßnahmen ist es, dass der komplette Lebenszyklus der Information komplett auditierbar ist. Die Verfügbarkeit von Gesundheitsinformationen ist schließlich wesentlich für die effektive Erbringung von Gesundheitsversorgung. Gesundheitssysteme müssen ganz besondere Anforderungen erfüllen, um im Falle einer Naturkatastrophe, eines Systemversagens und von Denial-of-Service-Attacken funktionsbereit zu bleiben. Deshalb erfordert der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsinformationen spezifisches Fachwissen aus dem Sektor des Gesundheitswesens.

Die Notwendigkeit eines effektiven IT-Sicherheitsmanagements in der Gesundheitsversorgung wird darüber hinaus aufgrund der wachsenden Nutzung von drahtlosen Technologien und von Internettechnologien bei der Erbringung von Gesundheitsversorgung immer dringender. Falls nicht ordnungsgemäß umgesetzt, werden diese komplexen Technologien das Risiko für Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsinformationen erhöhen. Unabhängig von Größe, lokaler Gegebenheiten und Modellen der Serviceerbringung müssen alle Organisationen der Gesundheitsversorgung über strikte Schutzmaßnahmen verfügen, um die ihnen anvertrauten Gesundheitsinformationen zu schützen. Derzeit arbeiten viele Heilberufler als Einzelanbieter von Gesundheitsdienstleistungen oder in kleinen Kliniken, die nicht die notwendigen IT Ressourcen haben, um Informationssicherheit zu managen. Organisationen der Gesundheitsversorgung müssen deshalb klare, eindeutige und für die Gesundheitsversorgung spezifisch angepasste Anleitungen für die Auswahl und Umsetzung solcher Schutzmaßnahmen haben. Diese Anleitungen müssen über einen weiten Bereich bezüglich Größe, lokaler Gegebenheiten und Modellen der Serviceerbringung in der Gesundheitsversorgung anzupassen sein. Letztlich – und auch in Hinblick auf den anwachsenden elektronischen Austausch von persönlichen Gesundheitsinformationen zwischen Heilberuflern – ist es ein klarer wirtschaftlicher Vorteil, eine gemeinsame Referenz für das Management von Informationssicherheit in der Gesundheitsversorgung anzuwenden.

ISO/IEC 27002 wird schon in großem Umfang über nationale oder regionale Leitlinien in Australien, Kanada, Frankreich, den Niederlanden, Neuseeland, Südafrika und im Vereinigten Königreich für das IT-Sicherheitsmanagement in der medizinischen Informatik genutzt. Auch in anderen Ländern wächst das Interesse. Die vorliegende internationale Norm (ISO 27799) stützt sich auf die Erfahrungen, die mit der Sicherheit persönlicher Gesundheitsinformationen in diesen nationalen Vorhaben gewonnen wurden und ist als begleitendes Dokument zur ISO/IEC 27002 gedacht. Sie ist nicht als Ersatz für ISO/IEC 27002 oder ISO/IEC 27001 gedacht. Sie ist vielmehr eine Ergänzung dieser eher generischen Normen.

ISO 27799 wendet ISO/IEC 27002 auf den Bereich der Gesundheitsversorgung an, wobei die angemessene Anwendung von Sicherheitsmaßnahmen zum Schutz persönlicher Gesundheitsinformationen sorgfältig betrachtet wird. Aufgrund dieser Betrachtungen haben die Autoren in einigen Fällen beschlossen, dass die Anwendung gewisser ISO/IEC 27002 Schutzziele wesentlich ist, falls persönliche Gesundheitsinformationen adäquat geschützt werden müssen. Deshalb führt die vorliegende Norm bei der Anwendungen einzelner in ISO/IEC 27002 spezifizierter Sicherheitsmaßnahmen Beschränkungen ein. Das wiederum hat bei einigen normativen Aussagen in Abschnitt 7 zu der Ergänzung geführt, dass die Anwendung einer vorgegebenen Sicherheitsmaßnahme verpflichtend ist. Zum Beispiel stellt 7.2.1 fest,

1) Diese Leitlinie ist konsistent mit der überarbeiteten Version von ISO/IEC 27002:2005.

*Organisationen, die Gesundheitsinformationen inklusive persönliche Gesundheitsinformationen verarbeiten, **müssen** eine schriftliche Leitlinie zur Informationssicherheit haben, die vom Management verabschiedet ist, veröffentlicht ist und dann allen Mitarbeiter und relevanten externen Parteien bekannt gegeben wird.*

Im Bereich des Gesundheitswesens kann eine Organisation (z. B. ein Krankenhaus) nach ISO/IEC 27001 zertifiziert werden, ohne dass eine Zertifizierung nach ISO 27799 oder auch nur die Kenntnis der ISO 27799 erforderlich ist. Es besteht allerdings die Hoffnung, dass – sowie Organisationen der Gesundheitsversorgung nach Verbesserung der Sicherheit persönlicher Gesundheitsinformationen streben – die Konformität mit der vorliegenden Norm – als der strikteren Norm für die Gesundheitsversorgung – sich weit verbreitet.

Alle Ziele der in ISO/IEC 27002 beschriebenen Sicherheitsmaßnahmen sind relevant für die medizinische Informatik, allerdings erfordern einige Maßnahmen ergänzende Erklärungen, wie diese am besten eingesetzt werden können, um Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsinformationen sicherzustellen. Darüber hinaus gibt es weitere gesundheitssektorspezifische Anforderungen. Die vorliegende internationale Norm ist eine ergänzende Anleitung in einer Form, die die Verantwortlichen für die Sicherheit von Gesundheitsinformationen einfach verstehen und anwenden können.

Die Autoren dieser Norm haben weder die Intention, eine Einführung in Computersicherheit zu schreiben, noch soll erneut festgeschrieben werden, was schon in ISO/IEC 27002 oder in ISO/IEC 27001 festgeschrieben wurde. Es gibt viele Sicherheitsanforderungen, die allen Computersystemen gemeinsam sind, unabhängig davon, ob sie nun für Finanzdienstleistungen, in der Produktion oder für Industriesteuerungen oder in irgendeinem ganz anderen organisierten Unternehmen eingesetzt werden. Es wurde ein konzertierter Vorstoß unternommen, um sich auf die Sicherheitsanforderungen zu fokussieren, die aufgrund der besonderen Herausforderungen bei der Bereitstellung elektronischer Gesundheitsinformationen zur Unterstützung der Erbringung von Pflegedienstleistungen benötigt werden.

Wer sollte diese internationale Norm lesen?

Diese internationale Norm ist an diejenigen gerichtet, die für die Überwachung der Sicherheit von Gesundheitsinformationen verantwortlich sind, und an Organisationen der Gesundheitsversorgung und Verwahrer von Gesundheitsinformationen, die zusammen mit ihren Sicherheitsberatern, Unternehmensberatern, Auditoren, Händlern und dritten Erbringern von Dienstleistungen eine Anleitung zu diesem Thema suchen.

Wirtschaftliche Vorteile bei der Anwendung dieser Norm

ISO/IEC 27002 ist eine umfassende und komplexe Norm, aber ihre Anweisungen sind nicht speziell auf die Gesundheitsversorgung abgestimmt. Die vorliegende Norm erlaubt die konsistente Umsetzung der ISO/IEC 27002 im Umfeld des Gesundheitswesens unter besonderer Berücksichtigung der speziellen Herausforderungen des Gesundheitswesens. Wenn Organisationen der Gesundheitsversorgung ihr folgen, helfen sie mit, dass Vertraulichkeit und Integrität der Daten in ihrem Pflegeumfeld gewahrt werden, dass kritische Gesundheitsinformationssysteme verfügbar bleiben, und dass die Zurechenbarkeit von Gesundheitsinformationen erhalten bleibt.

Die Anwendung dieser Anleitung von Organisationen der Gesundheitsversorgung, sowohl innerhalb von Rechtsprechungen als auch über Grenzen von Rechtsprechungen hinweg, ermöglicht die Unterstützung gemeinsamer Arbeitsabläufe und die sichere Anwendung neuer kollaborativer Technologien bei der Erbringung von Gesundheitsversorgung. Sichere und vertraulichkeitsschützende gemeinsame Nutzung von Informationen kann die Ergebnisse der Erbringung von Gesundheitsversorgung signifikant verbessern.

Als ein Ergebnis der Umsetzung dieser Anleitung können Organisationen der Gesundheitsversorgung erwarten, dass Anzahl und Schwere ihrer sicherheitsrelevanten Vorfälle zurückgehen, was wiederum erlaubt die vorhandenen Ressourcen wieder mehr für produktive Aktivitäten einzusetzen. Somit ermöglicht also IT-Sicherheit die kosteneffektive und produktive Nutzung von Ressourcen im Gesundheitswesen. In der Tat haben Untersuchung von Marktanalysten und des angesehenen Information Security Forums gezeigt, dass gute Rund-um-Sicherheit das Ergebnis von Organisationen um bis zu 2 % verbessern kann.

Letztlich wird ein konsistenter Ansatz zur IT-Sicherheit, der für alle in die Gesundheitsversorgung eingebundenen verständlich ist, das Betriebsklima verbessern und das öffentliche Vertrauen in Systeme, die persönliche Gesundheitsinformationen vorhalten, erhöhen.

Wie diese Norm genutzt werden sollte

Leser, die mit ISO/IEC 27002 noch nicht vertraut sind, sollten zunächst die einleitenden Abschnitte jener internationalen Norm lesen, bevor sie hier weiterlesen. Anwender dieser internationalen Norm (ISO 27799) müssen zunächst ISO/IEC 27002 ausführlich lesen, weil der folgende Text den Leser häufig auf relevante Abschnitte jener internationalen Norm verweist. Ohne den vollen Zugriff auf den Text von ISO/IEC 27002 kann das vorliegende Dokument nicht in vollem Umfang verstanden werden.

Allgemeine Leser, die mit Sicherheit von Gesundheitsinformationen sowie deren Zielen, Herausforderungen und dem weiteren Kontext noch nicht vertraut sind, profitieren von einer kurzen Einleitung in Abschnitt 5 dieses Dokuments.

Leser, die eine Anleitung suchen, wie ISO/IEC 27002 im Umfeld des Gesundheitswesens umzusetzen ist, finden in Abschnitt 6 eine praktische Anleitung. In dem Abschnitt sind keine verpflichtenden Anforderungen enthalten. Stattdessen werden allgemeine Ratschläge und Anleitungen gegeben, wie man am besten bei der Umsetzung von ISO/IEC 27002 in der Gesundheitsversorgung vorgeht. Der Abschnitt ist rund um einen Kreis von Aktivitäten (planen, ausführen, überprüfen, handeln) organisiert, der in ISO/IEC 27001 beschrieben ist und der, wenn er befolgt wird, zu einer soliden Umsetzung eines Informationssicherheits-Managementsystems führt.

Leser, die spezifische Anleitungen zu den in ISO/IEC 27002 beschriebenen elf Abschnitten mit Sicherheitsmaßnahmen und den 39 wesentlichen Kategorien von Sicherheitsmaßnahmen suchen, finden diese in Abschnitt 7. Dieser Abschnitt führt den Leser durch jeden der elf Abschnitte mit Sicherheitsmaßnahmen der ISO/IEC 27002. Es werden Mindestanforderungen aufgestellt, soweit angemessen, und in einigen Fällen werden normative Richtlinien zur ordnungsgemäßen Anwendung einzelner Sicherheitsmaßnahmen aus ISO/IEC 27002 zum Schutz von Gesundheitsinformationen dargelegt.

Diese internationale Norm schließt mit drei informativen Anhängen ab. Anhang A beschreibt die allgemeinen Bedrohungen von Gesundheitsinformationen. Anhang B beschreibt kurz Aufgaben und zugehörige Dokumente des Informationssicherheits-Managementsystems. Anhang C diskutiert die Vorteile von Tools als Hilfen bei der Umsetzung. Die Literaturhinweise führen verwandte Normen aus dem Bereich der Sicherheit von Gesundheitsinformationen auf.

1 Anwendungsbereich

1.1 Allgemeines

Diese internationale Norm gibt Richtlinien vor, um die Interpretation und Umsetzung der ISO/IEC 27002 (Information Technology – Security techniques – Code of practice for information security management) in der medizinischen Informatik zu unterstützen und ist ein begleitendes Dokument zu jener Norm²⁾.

Die vorliegende internationale Norm spezifiziert einen Satz detaillierter Maßnahmen zum Management der Sicherheit von Gesundheitsinformationen und stellt Best Practices Leitlinien zur Sicherheit von Gesundheitsinformationen zur Verfügung. Mit der Umsetzung dieser internationalen Norm ist es Organisationen der Gesundheitsversorgung und anderen Verwahrern von Gesundheitsinformationen möglich, ein minimal erforderliches Sicherheitsniveau sicherzustellen, das den Randbedingungen der Organisationen angemessen ist und das die Vertraulichkeit, Integrität und Verfügbarkeit von persönlichen Gesundheitsinformationen aufrecht erhält.

Diese internationale Norm gilt für Gesundheitsinformationen in all ihren Aspekten; denn in welcher Form auch immer die Informationen vorliegen (Worte und Zahlen, Tonaufzeichnungen, Abbildungen, Videomaterial und medizinische Bilder), welche Mittel auch immer zur Speicherung genutzt werden (auf Papier drucken oder schreiben oder elektrisches Speichern) und welche Mittel auch immer zur Übertragung genutzt werden (manuell, per Fax, über Computernetzwerke oder per Post), die Informationen müssen immer angemessen geschützt werden.

Diese internationale Norm definiert gemeinsam mit ISO/IEC 27002, was bezüglich Informationssicherheit in der Gesundheitsversorgung erforderlich ist; sie definieren nicht, wie diese Anforderungen zu erfüllen sind. Somit ist diese internationale Norm – so weit es irgendwie möglich ist – technologieneutral. Neutralität im Hinblick auf die Umsetzung von Technologien ist ein wesentliches Kennzeichen. Sicherheitstechnologien unterliegen immer noch einer schnellen Entwicklung und die Geschwindigkeit dieser Änderungen wird derzeit in Monaten und nicht in Jahren gemessen. Im Gegensatz dazu wird von Normen erwartet, auch wenn sie einer periodischen Überarbeitung unterliegen, dass sie im Großen und Ganzen für Jahre gültig bleiben. Ebenso wichtig ist, dass Technologieneutralität es Anbietern und Dienstleistern überlässt, neue oder sich entwickelnde Technologien anzubieten, die die in dieser internationalen Norm beschriebenen notwendigen Anforderungen erfüllen.

Wie in der Einleitung bereits festgehalten, ist die Kenntnis der ISO/IEC 27002 unverzichtbar für ein Verständnis dieser internationalen Norm.

1.2 Ausschlüsse aus dem Anwendungsbereich

Die folgenden Gebiete der Informationssicherheit liegen außerhalb des Anwendungsbereichs dieser internationalen Norm:

- a) Methoden und statistische Tests zur effektiven Anonymisierung persönlicher Gesundheitsinformationen;
- b) Methoden zur Pseudonymisierung persönlicher Gesundheitsinformationen (siehe Literaturhinweis [10] als Beispiel für eine ISO Technischen Spezifikation, die sich ganz speziell mit diesem Thema befasst);
- c) Quality of Service des Netzwerkes und Methoden, um die Verfügbarkeit von Netzwerken, die für die medizinische Informatik genutzt werden, zu messen; und
- d) Datenqualität (soweit nicht identisch mit Datenintegrität).

2) Diese Richtlinie ist konsistent mit der überarbeiteten Version von ISO/IEC 27002:2005.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 Begriffe aus dem Gesundheitswesen

3.1.1

medizinische Informatik

wissenschaftliche Fachrichtung, die sich mit den kognitiven, informationsverarbeitenden und kommunikativen Aufgabestellungen der Praxis, Ausbildung und Forschung in der Gesundheitsversorgung befasst, einschließlich der Informationswissenschaft und -technologie, um diese Aufgabenstellungen zu unterstützen

[ISO/TR 18307:2001, Definition 3.73]

3.1.2

Gesundheitsinformationssystem

Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen, in einer von Computern zu verarbeitenden Form, sicher gespeichert und übermittelt sowie zugänglich für mehrere autorisierte Nutzer

[ANMERKUNG Angepasst von ISO/TR 20514:2005 Definition 2.25.]

3.1.3

Gesundheitsversorgung

jegliche Art von Dienstleistungen mit Auswirkungen auf den Status der Gesundheit, die von Heilberuflern oder Hilfskräften erbracht wird

[Europäisches Parlament, 1998, wie von der WHO zitiert]

3.1.4

Organisation der Gesundheitsversorgung

allgemeiner Ausdruck, um viele Arten von Organisationen zu beschreiben, die Dienstleistungen der Gesundheitsversorgung erbringen

[ISO/TR 18307:2001, Definition 3.74]

3.1.5

Heilberufler

Person, die von einer anerkannten Stelle autorisiert ist, zur Erbringung gewisser medizinischer Dienstleistungen qualifiziert zu sein

[ANMERKUNG Angepasst von ISO/TS 17090-1:2002, Definition 3.18.]

3.1.6

Erbringer von Gesundheitsversorgung

jegliche Person oder Organisation, die in die Erbringung von Gesundheitsversorgung für einen Klienten eingebunden ist oder dazu gehört, oder die sich um das Wohlbefinden eines Klienten kümmert

3.1.7

identifizierbare Person

jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifizierungsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind

[ISO 22857:2004, Definition 3.7]

3.1.8

Patient

behandelte Person (siehe 3.1.10).

3.1.9

persönliche Gesundheitsinformationen

Informationen über eine identifizierbare Person, die sich auf den körperlichen oder geistigen Gesundheitszustand der betreffenden Person oder auf die Erbringung von Gesundheitsdienstleistungen für die betreffende Person beziehen, und zu denen folgende Informationen gehören können:

- a) Informationen über die Vormerkung der betreffenden Person zur Erbringung von Gesundheitsdienstleistungen,
- b) Informationen über Zahlungen oder Berechtigungen zum Empfang medizinischer Dienstleistungen bezüglich der betreffenden Person,
- c) eine Nummer, ein Symbol oder ein Kennzeichen, die/das einer bestimmten Person zugeteilt wurde, um diese für medizinische Zwecke eindeutig zu identifizieren,
- d) jegliche Informationen über die bestimmte Person, die im Rahmen der Erbringung von medizinischen Dienstleistungen erhoben wurde,
- e) Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz abgeleitet wurden, und
- f) Identifizierung einer Person (z. B. eines Heilberufers) als Erbringer von Gesundheitsversorgung für die bestimmte Person.

ANMERKUNG Persönliche Gesundheitsinformationen schließen Informationen nicht ein, die, entweder allein für sich oder in Kombination mit anderen Informationen, die für den Halter frei erhältlich sind, anonymisiert sind, d. h. die Identität der betroffenen Person, die Gegenstand der Informationen ist, kann aus den Informationen nicht abgeleitet werden.

3.1.10

behandelte Person

eine oder mehrere Personen, die terminlich eingeplant sind, eine Leistung des Gesundheitswesens zu erhalten, diese gerade erhalten oder diese bereits erhalten haben

[ISO/TS 18308:2004, Definition 3.40]

3.2 Begriffe aus dem Bereich der Informationssicherheit

3.2.1

Wert

alles, was für die Organisation von Wert ist

[ISO/IEC 13335-1:2004, Definition 2.2]

ANMERKUNG Im Kontext von Sicherheit von Gesundheitsinformationen umfassen die Werte:

- a) Gesundheitsinformationen
- b) IT-Dienstleistungen

- c) Hardware
- d) Software
- e) Kommunikationseinrichtungen
- f) Medien
- g) IT-Einrichtungen
- h) Medizinprodukte, die Daten aufzeichnen oder anzeigen.

3.2.2

Zurechenbarkeit

Eigenschaft, die gewährleistet, dass Aktionen einer Entität auch auf diese zurückgeführt werden können

[ISO 7498-2:1989, Definition 3.3.3]

3.2.3

Verlässlichkeit

Ergebnis einer Reihe von Prozessen zur Einhaltung von Vorgaben, durch die eine Organisation Vertrauen in den Zustand ihres Informationsmanagementsystems erwirbt

3.2.4

Verfügbarkeit

Eigenschaft, auf Nachfrage einer berechtigten Entität zugreifbar und verwendbar zu sein

[ISO 7498-2:1989, Definition 3.3.11]

3.2.5

Einschätzung der Einhaltung von Vorgaben

Prozesse, mit denen eine Organisation bestätigt, dass die eingesetzten Informationssicherheitsmaßnahmen sowohl funktionsbereit als auch wirksam sind

ANMERKUNG Einhaltung rechtlicher Vorgaben bezieht sich speziell auf die Sicherheitsmaßnahmen, die eingesetzt wurden, um die Anforderungen der relevanten Gesetzgebung, wie z. B. die Direktive der Europäischen Union zum Schutz persönlicher Daten, zu erfüllen.

3.2.6

Vertraulichkeit

Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder offenbart werden

[ISO 7498-2:1989, Definition 3.3.16]

3.2.7

Datenintegrität

Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind

[ISO 7498-2:1989, Definition 3.3.21]

3.2.8

Vorgaben zur Informationslenkung

Prozesse, durch die eine Organisation die Verlässlichkeit erhält, dass die Risiken für ihre Informationen, und damit auch die betrieblichen Möglichkeiten und die Integrität der Organisation, effektiv identifiziert und verwaltet werden

3.2.9

Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

ANMERKUNG Andere Eigenschaften, wie speziell die Zurechenbarkeit zu Nutzern, aber auch Authentizität, Nicht-Abstreitbarkeit und Verlässlichkeit werden oft als Aspekte der Informationssicherheit aufgeführt, können aber auch als von den drei Kerneigenschaften der Definition abgeleitet angesehen werden.

3.2.10

Risiko

Kombination aus Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen

[ISO Guide 73:2002, Definition 3.1.1]

3.2.11

Risikoeinschätzung

gesamter Prozess der Risikoanalyse und Risikobewertung

[ISO Guide 73:2002, Definition 3.3.1]

3.2.12

Risikomanagement

koordinierte Aktivitäten zur Leitung und Kontrolle einer Organisation in Bezug auf Risiken

ANMERKUNG Risikomanagement beinhaltet normalerweise Risikoeinschätzung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation.

[ISO Guide 73:2002, Definition 3.1.7]

3.2.13

Risikobehandlung

Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung (üblicherweise Reduktion) eines Risikos

ANMERKUNG Angepasst von ISO Guide 73:2002, Definition 3.4.1.

3.2.14

Systemintegrität

Eigenschaft, dass ein System seine vorgesehene Funktion in einer unbeeinträchtigten Art und Weise, frei von vorsätzlicher oder zufälliger unberechtigter Veränderung des Systems ausführt

3.2.15

Bedrohung

mögliche Ursache eines Vorfalles, der einem System oder einer Organisation einen Schaden zufügen kann

[ISO/IEC 13335-1:2004, Definition 2.25]

3.2.16

Schwachstelle

von einer oder mehreren Bedrohungen ausnutzbare Schwäche eines Wertes oder einer Gruppe von Gütern

[ISO/IEC 13335-1:2004, Definition 2.26]

4 Abkürzungen

ISMF	Informationssicherheits-Managementforum
ISMS	Informationssicherheits-Managementsystem
IT	Informationstechnologie
SLA	Service Level Agreement
SOA	Erklärung zur Anwendbarkeit (en: Statement of Applicability)

5 Sicherheit von Gesundheitsinformationen

5.1 Ziele für die Sicherheit von Gesundheitsinformationen

Vertraulichkeit, Verfügbarkeit und Integrität (einschließlich Authentizität, Zurechenbarkeit und Auditierbarkeit) von Informationen zu wahren sind die überragenden Ziele der Informationssicherheit. In der Gesundheitsversorgung, hängt die Privatsphäre der behandelten Person von der Wahrung der Vertraulichkeit persönlicher Gesundheitsinformationen ab. Um Vertraulichkeit zu wahren, müssen auch Maßnahmen zur Wahrung der Datenintegrität ergriffen werden, und sei es auch nur, weil es möglich ist, die Integrität von Zugriffskontrolldaten, Audit-Trails und anderen Systemdaten so zu verändern, dass Vertraulichkeitsverletzungen stattfinden können oder nicht wahrgenommen werden. Darüber hinaus hängt die Patientensicherheit von der Wahrung der Integrität persönlicher Gesundheitsinformationen ab; gelingt dies nicht, kann dies zu Krankheit, Verletzung oder sogar zum Tod führen. Ebenso ist eine hohe Verfügbarkeit eine besonders wichtige Eigenschaft medizinischer Systeme, da Behandlungen oft zeitkritisch sind. So können die Katastrophen, die zu Ausfällen anderer, nicht-medizinischer IT-Systeme führen können, genau die Situationen sein, in denen die in medizinischen Systemen enthaltenen Informationen am dringendsten benötigt werden. Darüber hinaus sind denial-of-service Attacken gegen vernetzte Systeme zunehmend normal.

Die in Abschnitt 7 diskutierten Maßnahmen wurden als für die Gesundheitsversorgung angemessen identifiziert, um Vertraulichkeit, Integrität und Verfügbarkeit persönlicher Gesundheitsinformationen zu schützen und sicherzustellen, dass der Zugriff auf solche Informationen auditiert und korrekt zugewiesen werden kann. Diese Maßnahmen helfen, Fehler in der medizinischen Behandlung zu vermeiden, die sich ergeben könnten, wenn die Integrität von Gesundheitsinformationen nicht gewahrt wurde. Zusätzlich helfen sie sicherzustellen, dass die Kontinuität medizinischer Dienstleistungen gewahrt bleibt.

Darüber hinaus gibt es weitere zu berücksichtigenden Sachverhalte, die die Ziele der Sicherheit von Gesundheitsinformationen beeinflussen. Dazu gehören:

- a) Anerkennung gesetzlicher Verpflichtungen, wie sie in einschlägigen Datenschutzgesetzen und Regelungen zum Schutz des Rechts des Patienten auf Privatsphäre dargelegt sind³⁾;
- b) Wahrung etablierter Best Practices für Privatsphäre und Sicherheit in der medizinischen Informatik;
- c) Wahrung individueller und organisatorischer Zurechenbarkeit über Grenzen von Organisationen im Gesundheitswesen hinweg und zwischen Heilberuflern;
- d) Unterstützung der Umsetzung eines systematischen Risikomanagements innerhalb von Organisationen im Gesundheitswesen;
- e) Erfüllung der Sicherheitserfordernisse, die in Routinesituationen der Gesundheitsversorgung identifiziert wurden;
- f) Reduzierung der Betriebskosten durch Erleichterung der zunehmenden Nutzung von Technologien in einer geschützten, sicheren und gut verwalteten Art und Weise, welche die laufenden Aktivitäten des Gesundheitswesens unterstützen – aber nicht einschränken – wird;
- g) Wahrung des öffentlichen Vertrauens in Organisationen im Gesundheitswesen und in die Informationssysteme, auf die sich diese Organisationen verlassen;
- h) Wahrung berufsspezifischer Standards und Ethikvorgaben, wie sie von berufsständischen Organisationen aus dem Bereich des Gesundheitswesens eingeführt wurden (soweit Informationssicherheit die Vertraulichkeit und Integrität von Gesundheitsinformationen sicherstellt);

3) Zusätzlich zu den gesetzlichen Verpflichtungen gibt es eine Fülle von Informationen über ethische Verpflichtungen in Bezug auf Gesundheitsinformationen, z. B. der Code of Ethics der Weltgesundheitsorganisation. Diese ethischen Verpflichtungen können unter gewissen Umständen auch die Leitlinie zur Sicherheit von Gesundheitsinformationen beeinflussen.

- i) Betrieb elektronischer Gesundheitsinformationssysteme in einer Umgebung, die angemessen gegen Bedrohungen geschützt ist;
- j) Erleichterung der Interoperabilität zwischen medizinischen Systemen untereinander, da Gesundheitsinformationen zunehmend über Grenzen von Organisationen und über juristische Grenzen hinweg fließen (speziell, da diese Interoperabilität den korrekten Umgang mit Gesundheitsinformationen unterstützt, um so deren kontinuierliche Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen).

5.2 Informationssicherheit als Teil der Vorgaben zur Informationslenkung⁴⁾

In den letzten Jahren sind Leitlinien zur Unternehmensführung als Antwort auf regulatorische Vorstöße wie den Sarbanes Oxley Act und den Health Insurance Portability and Accountability Act in den USA, die neue Europäische Baseler Eigenkapitalvereinbarung (Basel II), den britischen Turnbull Code und Deutschlands KontraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) zu einer kritischen Angelegenheit für Organisationen aller Art geworden. Ähnlich macht die wachsende Abhängigkeit der Organisationen von Informationen und den zugehörigen unterstützenden Technologien Vorgaben zur Informationslenkung zu einer wichtigen Komponente eines funktionierenden Risikomanagementprozesses.

Man kann davon ausgehen, dass viele Gebiete des Informationsmanagements, wie z. B. Akkreditierung und Datenschutz, in den Anwendungsbereich der Vorgaben zur Informationslenkung fallen. Es ist von vitaler Bedeutung, dass der Anwendungsbereich von Vorgaben zur Informationslenkung die fortlaufende Entwicklung der Informationssicherheit umfasst und unterstützt, so dass Vertraulichkeit, Integrität und Verfügbarkeit stets die gebührende Aufmerksamkeit gewidmet wird. Informationssicherheit ist eindeutig eine kritische Komponente, die dann die weiteren Aspekte der Vorgaben zur Informationslenkung ermöglicht.

5.3 Vorgaben zur Informationslenkung als Teil der unternehmerischen und klinischen Leitlinien

Während Organisationen im Gesundheitswesen in ihren Positionen bzgl. klinischer und unternehmerischer Leitlinien voneinander abweichen können, sollte – als vitale Unterstützung beider – die Notwendigkeit, Vorgaben zur Informationslenkung zu integrieren und zu befolgen, außer Frage stehen. So wie Organisationen im Gesundheitswesen in immer kritischerem Ausmaß von Informationssystemen zur Unterstützung der Pflege abhängig werden (z. B. durch sich entwickelnde Technologien zur Entscheidungsunterstützung und Trends zu ‚evidenzbasierter‘ anstelle von ‚erfahrungsbasierter‘ Gesundheitsversorgung), wird es zunehmend deutlich, dass Ereignisse, bei denen der Verlust von Integrität, Verfügbarkeit und Vertraulichkeit deutliche klinische Auswirkungen haben kann und dass daraus resultierende Probleme als Verfehlungen bezüglich der ethischen und rechtlichen Verpflichtungen, die dem Pflegeauftrag innewohnen, angesehen werden.

Es liegen zweifellos in allen Ländern und Rechtsprechungen Fallstudien vor, nach denen solche Pflichtverletzungen zu Missdiagnosen, Tod oder verzögerter Heilung geführt haben. Die Rahmenwerke für die klinische Leitung müssen deshalb effektives Risikomanagement zur Informationssicherheit mit derselben Bedeutung behandeln wie Pflegepläne, Infektionsmanagementstrategien und andere ‚Kern‘themen des klinischen Managements.

4) Es ist zu beachten, dass die Vorgaben zur Informationslenkung in einigen Ländern als Verlässlichkeit von Informationen bezeichnet wird.

5.4 Zu schützende Gesundheitsinformationen

Es gibt mehrere Arten von Informationen, deren Vertraulichkeit, Integrität und Verfügbarkeit⁵⁾ geschützt werden muss:

- a) persönliche Gesundheitsinformationen,
- b) pseudonymisierte Daten, die mit Hilfe gewissen Methoden zur Pseudonymisierung von persönlichen Gesundheitsinformationen abgeleitet wurden,
- c) statistische Daten und Forschungsdaten, inklusive anonymisierter Daten, die von persönlichen Gesundheitsinformationen durch Entfernen der persönlich identifizierenden Daten abgeleitet wurden,
- d) klinisches/medizinisches Wissen, das sich nicht auf eine beliebige aber spezifische, behandelte Person bezieht, inklusive Daten zur Unterstützung klinischer Entscheidungen (z. B. Daten über ungünstige Arzneimittelreaktionen),
- e) Daten über Heilberufler, Personal und Freiwillige,
- f) Informationen zur öffentlichen Gesundheitsüberwachung,
- g) Daten aus Audit-Trails medizinischer Informationssysteme, die persönliche Gesundheitsinformationen oder pseudonymisierte Daten, die von persönlichen Gesundheitsinformationen abgeleitet wurden, enthalten oder die Daten über Aktionen von Nutzern im Hinblick auf persönliche Gesundheitsinformationen enthalten,
- h) Sicherheitsdaten von Gesundheitsinformationssystemen, inklusive Daten zu Zugriffsregelungen und andere sicherheitsbezogene Systemkonfigurationsdaten für Gesundheitsinformationssysteme.

Das Ausmaß, in dem Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden müssen, hängt von der Natur der Informationen, deren Nutzung und den Risiken, denen sie ausgesetzt sind, ab. Beispielsweise sind statistische Daten [siehe Punkt c) oben] zwar nicht unbedingt vertraulich, aber der Schutz ihrer Integrität kann sehr wichtig sein. Ebenso erfordern Daten aus Audit-Trails [siehe Punkt g) oben] nicht unbedingt eine hohe Verfügbarkeit (regelmäßiges Archivieren mit einer in Stunden statt in Sekunden zu messenden Zugriffszeit müsste bei einer vorgegebenen Anwendung ausreichen), aber ihr Inhalt kann hoch vertraulich sein. Eine Risikoeinschätzung kann den zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit notwendigen Schutz angemessen bestimmen (siehe 6.4.4). Die Ergebnisse regelmäßiger Risikoeinschätzungen müssen an die Prioritäten und Ressourcen der umsetzenden Organisation angepasst werden.

5.5 Bedrohungen und Schwachstellen der Sicherheit von Gesundheitsinformationen

Die Arten der Informationssicherheitsbedrohungen und -schwachstellen variieren stark, wie auch deren Beschreibungen. Während eigentlich keine wirklich einzigartig für die Gesundheitsversorgung ist, ist es die Menge an Faktoren, die bei der Einschätzung von Bedrohungen und Schwachstellen berücksichtigt werden muss, die einzigartig für die Gesundheitsversorgung ist.

Es liegt in der Natur der Sache, dass Organisationen im Gesundheitswesen in einer Umgebung arbeiten, aus der Besucher und die Öffentlichkeit niemals gänzlich ausgeschlossen werden können. In großen Organisationen im Gesundheitswesen ist allein schon die Menge an Personen, die sich durch Funktionsbereiche bewegen, signifikant. Diese Faktoren erhöhen die Verletzlichkeit von Systemen bezüglich physischer Bedrohungen. Die Wahrscheinlichkeiten, dass solche Bedrohungen auch tatsächlich eintreten, können weiter ansteigen, wenn emotionell oder geistig kranke behandelte Personen oder Angehörige anwesend sind.

5) Das Niveau der Verfügbarkeit hängt von der vorgesehenen Nutzung der Daten ab.

Viele Organisationen im Gesundheitswesen sind chronisch unterfinanziert und ihr Personal muss unter signifikantem Stress arbeiten. Dies kann sich oft in erhöhten Fehlerraten inkl. der Durchführung unkorrekter Behandlungen widerspiegeln. Als weitere Folge solcher Ressourcenzwänge gibt es Systeme, die in äußerst nachlässiger Art und Weise entworfen, implementiert und betrieben werden, oder Systeme, die weiterhin betrieben werden, obwohl sie schon längst außer Dienst gestellt werden sollten. Diese Faktoren können die Anfälligkeit für gewisse Bedrohungstypen erhöhen und Verletzlichkeiten verschlimmern. Auf der anderen Seite ist klinische Pflege immer noch ein Prozess, der eine ganze Reihe von speziell ausgebildetem, technischem, verwalterisch tätigem, zuarbeitendem und freiwilligem Personal einbezieht, von denen viele ihre Arbeit als Berufung sehen. Deren Hingabe und deren Bandbreite an Erfahrungen kann oft auf nützliche Art und Weise die Bloßstellung von Schwachstellen begrenzen. Auch das hohe Niveau der beruflichen Ausbildung vieler Heilberufler grenzt die Gesundheitsversorgung von vielen anderen Industriebranchen ab, so dass Insiderbedrohungen seltener vorkommen.

Die kritische Notwendigkeit, behandelte Personen korrekt zu identifizieren und sie ihren Gesundheitsakten korrekt zuzuordnen, führt dazu, dass Organisationen im Gesundheitswesen detailliert identifizierende Informationen erheben. Regionale oder einen Rechtsraum betreffende Patientenregister (d. h., Register von behandelten Personen) sind manchmal die umfassendsten und aktuellsten Ablagen identifizierender Informationen, die in einem Rechtsraum verfügbar sind. Diese identifizierenden Informationen sind von großem potentielltem Wert für „Identitätsdiebstähle“ und müssen deshalb streng geschützt werden.

Das Umfeld des Gesundheitswesens mit seinen besonderen Bedrohungen und Verletzlichkeiten sollte deshalb mit spezieller Sorgfalt betrachtet werden. Anhang A enthält eine informative Liste von Bedrohungstypen, die von Organisationen im Gesundheitswesen bei der Einschätzung von Risiken für Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsinformationen sowie von Risiken für Integrität und Verfügbarkeit der zugehörigen Informationssysteme zu berücksichtigen sind.

6 Praktischer Arbeitsplan für die Umsetzung der ISO/IEC 27002

6.1 Systematik der Normen ISO/IEC 27002 und ISO/IEC 27001

ISO/IEC 27002 stellt eine standardisierte Checkliste von Schutzzielen für 11 Sachgebiete bereit, die insgesamt 39 wesentliche Sicherheitskategorien enthalten, jede mit einer Beschreibung von einer oder mehrerer Sicherheitsmaßnahmen. Wer ISO/IEC 27002 im Umfeld des Gesundheitswesens umsetzt, wird feststellen, dass die meisten Schutzziele in fast allen Situationen anwendbar sind. Allerdings müssen Anwender der Norm in der Gesundheitsversorgung auch anerkennen, dass es Situationen gibt, in denen zusätzliche Schutzziele erforderlich sein können. Das ist oft der Fall, wenn sich klinische Prozesse mit der Nutzung spezieller Geräten, wie Scannern, Infusionspumpen o. ä., überschneiden, selbst wenn sich die Sicherheitsmaßnahmen nur auf die Wahrung der Unversehrtheit der Gerätedaten beziehen. Darüber hinaus werden unterschiedliche Rechtsprechungen auch unterschiedliche rechtliche Rahmenbedingungen setzen, die den erforderlichen Anwendungsbereich von Aktivitäten zur Einhaltung von Vorgaben ändern können.

ISO/IEC 27001 führt das Konzept eines 'Informationssicherheits-Managementsystems (ISMS)' ein und beschreibt die Notwendigkeit für diesen detaillierten Rahmen von Maßnahmen, wenn Anstrengungen gemacht werden, um die Sicherheitsmaßnahmen zu erfüllen, die vom Risikomanagement als relevant aufgezeigt wurden. Internationale Erfahrungen und anerkannte Best Practices Prinzipien zeigen an, dass die kontinuierliche Erfüllung der ISO/IEC 27002 am besten durch die Umsetzung eines in Bild 1 abgebildeten Managementsystems sichergestellt werden kann.

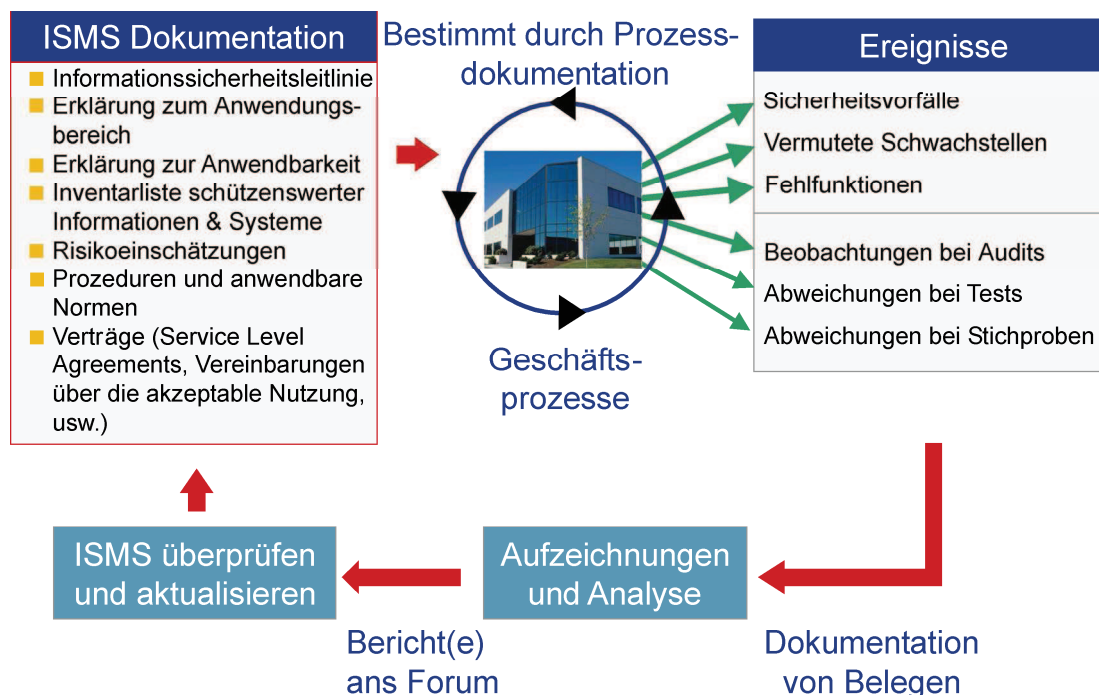


Bild 1 — Das Informationssicherheits-Managementsystem

Organisationen im Gesundheitswesen sollten, soweit möglich, ihr ISMS in die Prozesse für Vorgaben zur Informationslenkung, die in 5.2 und 5.3 beschrieben sind, integrieren und sollten dabei die Anleitung, die in den Abschnitten 6.2 bis 6.7 gegeben wird, berücksichtigen.

Ein üblicher Fehler, der speziell von öffentlichen Organisationen im Gesundheitswesen gemacht wird, bei denen es typischerweise keine zentrale Anforderungen zur formalen Akkreditierung oder Zertifizierung gibt, ist es, die Einhaltung der ISO/IEC 27002 als reine Abarbeitung einer Checkliste zu beschreiben. Um sie tatsächlich einzuhalten, müssen Organisationen in der Lage sein, ein einsatzbereites ISMS vorzuweisen, in dem es angemessene Prozesse zur Auditierung der Einhaltung von Anforderungen gibt. Diese Einhaltung von Vorgaben passt gut zusammen mit dem regulatorischen Rahmenwerk, in dem Organisationen im Gesundheitswesen typischerweise arbeiten. Siehe auch 7.12.

6.2 Engagement des Managements bei der Umsetzung der ISO/IEC 27002

Es ist wesentlich, dass eine Organisationen im Gesundheitswesen die eindeutige Unterstützung des Managements erhält, bevor sie versucht ISO/IEC 27002 einzuhalten. Es ist klar, dass die aktive Einbeziehung und die Unterstützung des Managements für den Erfolg wesentlich sind. Diese Einbeziehung sollte schriftliche und mündliche Aussagen zum Engagement bezüglich der Wichtigkeit der Sicherheit von Gesundheitsinformationen und der Anerkennung ihrer wirtschaftlichen Vorteile enthalten.

Eine Risikoeinschätzung ist eine gute Gelegenheit, um ernste Risiken zu entdecken, die wiederum gründliche Veränderung an existierenden Prozessen erfordern, um eben diese Risiken zu mindern. Der persönliche Wille des Managements, sich selbst und die Organisation Prozessänderungen zu unterwerfen und Wegbereiter für solche Veränderungen zu sein, muss eindeutig gezeigt werden.

Ohne diese ersten Schritte, wird das Engagement anderer unvollständig bleiben. Unnötige Vermutungen über den "wirklichen Zweck" des Programms (z. B., wird es umgesetzt, um die Wirksamkeit der Informationssicherheit zu erhöhen oder um die Anzahl der benötigten Mitarbeiter zu verringern?) können unter den Stakeholdern aufkommen.

Darüber hinaus muss das Management darauf vorbereitet sein, dass mit einiger Wahrscheinlichkeit die kurzfristige Steigerung von Ausgaben, die aufgrund des Übergangs zu den neuen Prioritäten wahrscheinlich ist, speziell im Gesundheitswesen negative Kommentare hervorruft. Solche Kommentare können auch aus einer Mischung von Wahrnehmungen über den Zweck und die dazu gehörenden Pläne herrühren. Ein klares Engagement des Managements kann solcherlei Probleme minimieren.

6.3 Einrichten, betreiben, pflegen und verbessern des ISMS

Die vier folgenden Unterabschnitte bieten eine Anleitung zum Einrichten und nachfolgenden Betreiben eines ISMS im Umfeld des Gesundheitswesens. Dies erfordert, wie in Bild 2 beschrieben, die zyklische Abarbeitung von Aktivitäten.

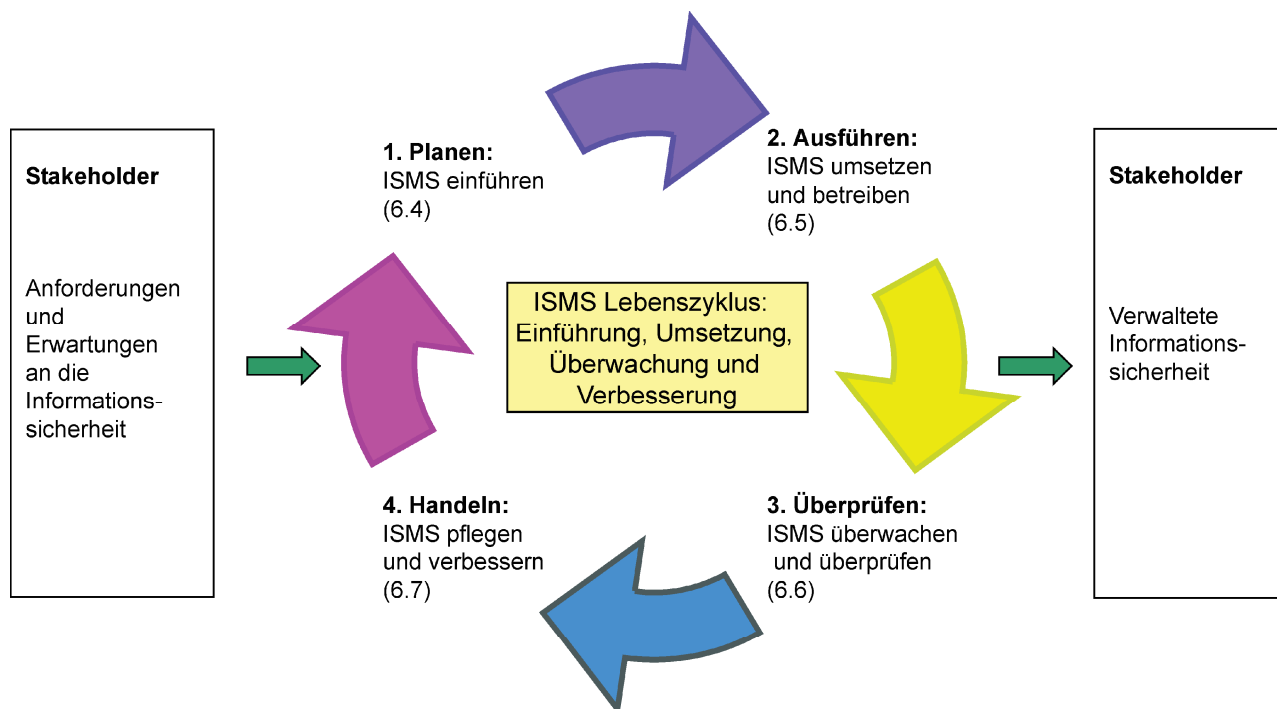


Bild 2 — Überblick über den ISMS-Prozess

Anhang B gibt informative Beispiele zu den Schritten, die typischerweise zu den einzelnen Phasen des Lebenszyklus gehören, zusammen mit Beispielen der Arten von Dokumenten, die in den einzelnen Phase benötigt werden.

6.4 Planen: Einführen des ISMS

6.4.1 Auswahl und Definition des Anwendungsbereiches

6.4.1.1 Allgemeines

Theoretisch kann ISO/IEC 27002 auf komplette Organisationen angewendet werden. Allerdings haben die Erfahrungen von Umsetzungen im Vereinigten Königreich gezeigt, dass sehr große Organisationen Schwierigkeiten haben, die dazu gehörenden Arbeiten abzuschließen und den notwendigen Grad der Einhaltung von Vorgaben in einem Anlauf zu realisieren.

Es hat sich herausgestellt, dass dies bei Anwendungsbereichen, die nicht mehr als 2 oder 3 Standorte oder ungefähr 50 Mitarbeiter oder ungefähr 10 Prozesse umfassen, sehr gut funktioniert. Aus diesen Gründen sind Ersthelferpraxen, Polikliniken, Teams für Hausbesuche, Spezialkliniken und Direktionen wirksame Anwendungsbereiche. Typischerweise wird ein inkrementeller und iterativer Prozess verfolgt, um eine vollständige Abdeckung zu erreichen und alle wirtschaftlichen Vorteile zu realisieren. Die Aussichten, solche Ergebnisse zu erreichen, sollten nicht durch die Auswahl eines überaus breiten Anwendungsbereiches unterminiert werden. Wo allerdings Dritte als IT-Dienstleister beschäftigt sind, wurde der Anwendungsbereich "Management der Bereitstellung von IT-Dienstleistungen" in großem Umfang mit beachtenswertem Erfolg festgelegt.

In Organisationen im Gesundheitswesen, wie auch anderswo, haben die Aktivitäten der vergangenen Jahre die Informationssicherheit erfolgreich von einer "Back-Office"-Funktion zu einer bekannten zentralen Verantwortlichkeit gemacht.

In der Gesundheitsversorgung macht die umfassende gegenseitige Abhängigkeit von Funktionen die Definition des Anwendungsbereiches zu einer Herausforderung. Aus diesem Grund ist es besonders wichtig, dies korrekt zu tun.

6.4.1.2 Kriterien zur Definition des Anwendungsbereiches

Um die "Bereitstellbarkeit" der Einhaltung von Vorgaben gegenüber den zentralen wirtschaftlichen Vorteilen angemessen abzuwägen, haben viele Organisationen des öffentlichen Sektors, inklusive Organisationen im Gesundheitswesen, die „sichere Bereitstellung von IT-Dienstleistungen“ als anfänglichen Anwendungsbereich definiert. Obwohl eher auf die Infrastruktur als auf die Geschäftsprozesse bezogen, überträgt dieser Anwendungsbereich reale zentrale wirtschaftliche Vorteile in dem Sinne, als er kritische Aufgaben vollendet, inklusive Absicherung der Infrastruktur als Ganzes, Anregung der Einspielung aller benötigten Aktualisierungen der zentralen Sicherheitsprozessen und Verbesserung des Identitätsmanagements, des Bewusstseins für Informationssicherheit und des Managements zur Aufrechterhaltung des Geschäftsbetriebs. Typischerweise werden sich auf vielen dieser Felder zentrale wirtschaftliche Vorteile über den gewählten Anwendungsbereich hinweg und über den gewählten Anwendungsbereich hinaus ergeben.

Deshalb ist es wesentlich, dass Kriterien zur Definition des Anwendungsbereichs benutzt werden. Die Kriterien sind typischerweise von "weicher" Art und umfassen Themen wie:

- a) das Ausmaß der angestrebten Sichtbarkeit;
- b) das angestrebte Verhältnis der geschäftlichen und fachlichen Zusammenarbeit;
- c) das angestrebte Ausmaß der lokalen oder zentralen Bedeutung;
- d) das Ausmaß der Handhabbarkeit, das der Anwendungsbereich einführt.

6.4.1.3 Mögliche zusammenfassende Gap Analyse zur Definition des Anwendungsbereichs

Bevor der Anwendungsbereich endgültig ausgewählt wird, kann es angebracht sein, beispielhaft eine Gap Analyse durchzuführen, um dadurch vor der endgültigen Auswahl ein "Gefühl" zu bekommen, wie viel Arbeit die einzelnen Arbeitsgebiete erzeugen können. Ob ein "leichtes" oder "schweres" Arbeitsgebiet gewählt wird, ist dabei Sache der Organisation, obwohl logischerweise bei der Bearbeitung der "harten" Aspekte des Anwendungsbereichs entsprechend mehr zentraler wirtschaftlicher Vorteil gewonnen wird.

6.4.1.4 Geregelte Einbeziehung Dritter

Ein anderes Gebiet, in dem typischerweise Fehler gemacht werden, ist die Interpretation des Anwendungsbereiches. Der Anwendungsbereich beinhaltet die von Dritten erbrachten Dienstleistungen und die Erbringung der erforderlichen Unterstützungsprozesse, aber keine Festlegung, wie diese Unterstützungsprozesse erbracht werden.

6.4.1.5 Service Level Agreements (SLAs) und Verträge helfen den Anwendungsbereich festzulegen

SLAs und Verträge können auch bei der Definition des Anwendungsbereichs helfen, so weit diese Instrumente wirkungsvoll die Grenzen des Anwendungsbereichs definieren. Selbst falls sie dies natürlich in einigen Fällen nicht tun, wird es immer noch wertvoll sein, sie zu überprüfen, um mögliche Prioritäten für Verbesserungen zu klären.

6.4.1.6 Erarbeitung und Verteilung der Erklärung des Anwendungsbereichs

Eine formale Erklärung zum Anwendungsbereich muss erarbeitet werden, speziell wenn eine Zertifizierung nach ISO/IEC 27001 angestrebt wird. Die Erklärung soll in der Organisation weiträumig veröffentlicht werden. Es ist wichtig, dass die Erklärung zum Anwendungsbereich die Grenzen der Aktivitäten zur Einhaltung von Vorgaben in Bezug auf Mitarbeiter, Prozesse, Orte, Plattformen und Anwendungen definiert.

Im Fall von Organisationen im Gesundheitswesen, sollte die Erklärung von den Gruppen, die Vorgaben zur Informationslenkung, zu klinischen Leitlinien und zu unternehmerischen Leitlinien machen, weiträumig veröffentlicht, überarbeitet und angewendet werden. Tatsächlich ist von einigen Organisationen im Gesundheitswesen bekannt, dass sie Kommentare zu dieser Erklärung von regulatorisch relevanten berufsständischen Organisationen aus dem Umfeld des Gesundheitswesens gesucht haben, die wiederum Kenntnis hatten von anderen Organisationen, die nach der Einhaltung von Vorgaben oder Zertifizierung strebten.

7.3.2.1 enthält Mindestanforderungen an Erklärungen zum Anwendungsbereich.

6.4.2 Gap Analyse

Sobald der Anwendungsbereich festgelegt ist, ist der nächste Schritt des Planungsprozesses eine Gap Analyse, in der eine grobe Bewertung der Einhaltung der Vorgaben durchgeführt wird. Best Practice hat gezeigt, dass der Fokus dieser Analyse auf die organisatorische Verantwortlichkeit, Umsetzung, Dokumentation von Sicherheitsverfahren und die Erkenntnisse, die zur Unterstützung der Analyse genutzt werden, gelegt werden muss. Das ist eindeutig in Übereinstimmung mit dem Vorgehen im Gesundheitswesen, wo angemessene Kenntnisse, Aufzeichnungen und Verfahren wichtig sind.

Ein üblicher Fehler solcher Analysen ist es, keine vergleichenden Ansichten und Bestätigungen zu erhalten. Der Analyst riskiert, dass er Kommentare erhält, die allein die Hoffnungen einiger Personen anstelle eines stimmigen Eindrucks der gängigen Verfahren wiedergeben. Er muss sich die Zeit nehmen, um Heilberufler und Manager zu befragen, um letztlich einen gut abgerundeten Eindruck zu erhalten.

Der Zweck der Gap Analyse ist es, eine erste Anleitung für erforderliche Verbesserungen, in Bearbeitung befindliche detaillierte Auswertungen der Risikoeinschätzung (siehe 6.4.5.1) und Risikobehandlung (siehe 6.4.5.2) zu geben. Außerdem kann die Gap Analyse eine erste Priorisierung für solche Verbesserungen vorschlagen.

6.4.3 Einrichtung oder Erweiterung eines Forums zur Sicherheit von Gesundheitsinformationen

Als Herzstück des ISMS muss ein angemessenes Informationssicherheits-Managementforum (ISMF) eingerichtet werden, um Informationssicherheit als Ganzes zu überblicken und zu leiten. Was "angemessen" bedeutet, variiert von Organisation zu Organisation und wird auch über das Spektrum der Gesundheitsversorgung hinweg variieren.

Die Strukturierung des Forums wird eine Herausforderung sein, da die Ansichten vieler Stakeholder berücksichtigt werden müssen und viele regulatorische Verpflichtungen erfüllt werden müssen. So wie die Funktionen des ISMF nicht abgewälzt oder noch weiter verteilt werden können, ohne Wirksamkeit zu verlieren, so sollte auch die Schaffung des ISMF nicht genutzt werden, um "noch ein weiteres Komitee" zu gründen. Es ist üblicherweise besser, den Fokus eines existierenden Komitees, wie z. B. eines, dass Risiken behandelt oder die Vorgaben zur Informationslenkung zur Aufgabe hat, zu erweitern.

Die Mitglieder müssen den vollen Bereich der Funktionen zur Verlässlichkeit von Informationen und der Funktionen zu den Vorgaben zur Informationslenkung umfassen, ebenso wie Vertreter unterschiedlicher Nutzerverbände und Vertreter der wesentlichen Unterstützungsfunktionen. Vertreter der internen Revision (Internes Audit) und der Personalabteilung sind ebenfalls typischerweise anwesend.

Der (virtuelle oder reelle) Informationssicherheitsbeauftragte der Organisation sollte, neben anderen Verpflichtungen, an das Forum berichten und es mit Assistenzdienstleistungen unterstützen und sollte weiterhin für das Zuordnen, Veröffentlichen und Kommentieren der Berichte, die von Mitgliedern des Forums entgegengenommen wurden, verantwortlich sein.

Wie in 5.2 und 5.3 beschrieben, macht die zentrale Natur der Informationssicherheit innerhalb der Lenkung von Informationen die Positionierung des ISMF innerhalb der Strukturen zur Lenkung von Informationen zu einer sehr vernünftigen Anordnung, aber nur, wenn im Gegenzug die letzte Gruppe mit der klinischen Leitungsstruktur verbunden ist. Klinische Leitlinien haben mit Aspekten der Patientensicherheit zu tun und diese sind oft sehr eng mit den Sicherheitsaspekten von Gesundheitsinformationen verbunden, zu denen die Vorgaben zur Informationslenkung gehören muss.

Wenn man den Ansatz nimmt, Vorgaben zur Lenkung von Informationen zu machen, so unterstreicht dies die kritische Natur von Informationssicherheit und erlaubt darüber hinaus einen integrierten Prozess, bei dem die Risikoanalyse direkt Input in die klinische Führung einfließen lässt. Die Beseitigung des „Schubkasten-denken“, das Informationssicherheit, Datenschutz, Informationsfreiheit, usw. separiert, kann nur helfen, doppelte Kosten zu beseitigen und gesteigerte Verlässlichkeit der Prozessintegrität zu liefern.

6.4.4 Risiken für Gesundheitsinformationen einschätzen

6.4.4.1 Allgemeines

Die Risikoeinschätzung ist der Mechanismus, durch den der Rahmen der Maßnahmen, der die ISO/IEC 27002 Schutzziele liefert, identifiziert werden muss. Dieser Prozess ist gut in der ISO/IEC TR 13335-3 dokumentiert.

Es gibt eine Anzahl spezieller Betrachtungen im Gesundheitsumfeld, die es wert sind, diskutiert zu werden.

6.4.4.2 Die Rolle der Einschätzung des Informationssicherheitsrisikos in der Gesundheitsversorgung

Die Gesundheitsversorgung bringt eindeutig relativ hohe Risiken mit sich, ganz speziell in solchen Gebieten wie Labor, Notfallabteilungen und Operationsräumen. Eine Abweichung mit geringem Risiko in Aktivitäten im Zusammenhang mit Gesundheitsinformationen, die solche Gebiete unterstützen, sollte deshalb hinterfragt werden, obwohl die Fehlannahme, dass jede Aktivität im Zusammenhang mit Gesundheitsinformationen direkt mit der Erbringung medizinischer Dienstleistungen verbunden ist, genauso falsch wäre.

Einschätzungen des Informationssicherheitsrisikos in der Gesundheitsversorgung sollten sowohl qualitative als auch quantitative Faktoren berücksichtigen. Finanzielle Verluste sollten nicht vorrangig Berücksichtigung finden, können aber dort berücksichtigt werden, wo es Erkenntnisse gibt, dass große Summen für Kleinigkeiten gezahlt wurden. Eine sorgfältige Gestaltung von Bewertungs-Richtlinien, die relevant für Gesundheitsversorgung sind, werden erforderlich sein, z. B. Richtlinien, die die Bedeutung von Patientensicherheit, ununterbrochener Verfügbarkeit von Notfalldienstleistungen, berufsständischer Akkreditierung und klinischer Vorgaben anerkennen.