DIN EN ISO 27799:2008-10 (D)

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

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 Unterstüzungs-Tools** ... 65

Literaturhinweise ... 68