MAS IS 19

Fallstudie

„Risikomanagement (Anwendung ISMS)“ – Aufgabenstellung und Bearbeitungsplan

Dozierende:
Hans-Peter Königs, IT Risk KM Consulting GmbH / koenigs@it-risk.ch
Marcus Griesser, SBB AG / marcus.griesser@sbb.ch

Version 2.0

Mai 2014

1 Inhalt

2 Generelle Bemerkungen zur Fallstudienbearbeitung

2.1 Ziele der Fallstudienbearbeitung

- Erlernen bzw. Vertiefen des Umgangs mit prozessorientierten Standards und deren praktischen Anwendung - hier im Besonderen die Standards ISO/IEC 27001:2013 (ISMS[1]), ISO/IEC 27002:2013, ISO/IEC 27003:2010 und ISO/IEC 27005:2011.
- Erstellung eines Vorgehensplans und eines Einführungskonzepts zur Einführung eines ISMS auf der Basis von ISO/IEC 27001:2013 unter zwingender Berücksichtigung des Risikoansatzes sowie des anschliessenden Betriebs des zu implementierenden ISMS.
- Erstellung eines Ausblickes auf einen KVP[2], um die Qualität des ISMS Prozesses, sowie dessen Ergebnisse fortlaufend zu verbessern.
- Sukzessive, prozessorientierte Bearbeitung der Fallstudie gemäss den gestellten Aufgaben anhand von nachvollziehbaren, bewertbaren Grundlagendokumenten.
- Berücksichtigung der möglichen Einflussfaktoren, z.B. Anforderungen aus sozialen, rechtlichen, organisatorischen und technologischen Aspekten. Dabei sind besonders die in einem Spitalumfeld *wichtigen rechtlichen Anforderungen* in die Risiko-Bewertungen und Massnahmengestaltungen einzubeziehen.
- Aufzeigen kritischer Trade-offs zwischen Standard und umsetzbarer Realität.
- Austausch der Gruppen untereinander zur Erzielung einer möglichst breiten Abdeckung der wichtigsten Geschäftsprozesse des Spitals innerhalb einer begrenzten Fallstudien-bearbeitungszeit.
- Erstellung und Durchführung einer managementgerechten Präsentation, aus der verständlich, überzeugend und nachvollziehbar das Einführungskonzept mit seinen Anforderungen, nachhaltigen Leistungen und betrieblichen Konsequenzen (einschl. der Aufwände und Kosten für die nächsten 3 Jahre) hervorgeht.

2.2 Rahmenbedingungen

Folgende Rahmenbedingungen sind dabei zu beachten:

- Die Kursleitung und die durchführenden Dozenten gehen davon aus, dass die Studierenden sowohl mit praktischer Konzeptarbeit als auch mit wissenschaftlicher Themenbehandlung vertraut sind und erwarten eine hohe Eigenverantwortung und ein hohes Engagement bei der Bearbeitung der Fallstudie.
- Jede Gruppe muss mindestens zwei der aus der Fallbeschreibung hervorgehenden Businessprozesse bearbeiten. Zur möglichst vollständigen Bearbeitung der wichtigsten Businessprozesse des Falles stimmen die Gruppen die Aufteilung der Business-Prozesse vorgängig untereinander ab. Eine aus früheren Analysen stammende Zusammenstellung von wichtigen Business-Prozessen ist in Anhang 1 aufgeführt.

[1] Information Security Management System (ISMS)

[2] Kontinuierlicher Verbesserungsprozess (KVP)

- Es wird erwartet, dass Sie sich bei der Fallstudienbearbeitung vor allem an etablierte Methoden und Standards halten, z.B. den PDCA-Zyklus und die relevanten Standards, Gesetze und Regulativen. Verbindliche Referenzen für Ausarbeitungen sind die Standards ISO/IEC 27001:2013 und ISO7IEC 27002:2013.
- Alle im Rahmen der Fallstudienbearbeitung erstellten Unterlagen und Ergebnisse sind den Dozenten am Präsentationstag, vor der Präsentation, in elektronischer Form (auf USB-Stick, CD, o.ä.) zur Bewertung zur Verfügung zu stellen.

2.3 Ausgangslage zur Fallbearbeitung

Ihre Gruppe ist ein fiktives Beraterteam der Firma „MAS-Risk & Security Consulting AG“ und bereits vertraut mit der Firma Sanamed, da sie bereits Mandate für Sanamed ausgeübt hat. Sie arbeiten eng mit dem Informationssicherheitsbeauftragten (ISO) der Sanamed zusammen.

Im Rahmen eines internen Audits bei der Sanamed mit Fokus auf das Interne Kontrollsystem (IKS), wurde u.a. bemängelt, dass …

- keine Konzeption bezüglich der Definition und Implementation eines ISMS gefunden werden konnte.

Weiter bemängelte der Auditor, dass …

- für die vorhandenen Sicherheits-Controls keine Dokumentation besteht, welche die im Gesamtkontext massgeblichen Risiko-Überlegungen darlegen würde und
- die Verantwortlichkeiten für die Informationssicherheit unklar sind.

Der Informationssicherheitsbeauftragte (ISO) der Sanamed akzeptiert die oben erwähnten Audit-Findings und beauftragt Sie, an die Adresse der Geschäftsleitung, ein Konzept zur Definition und Implementation eines ISMS bei der Sanamed (inkl. der dazugehörigen Hintergrundinformationen wie Vorgehen, Planungen, Templates mit jeweils einigen Beispielen) auszuarbeiten.

Anmerkung: Für die Umsetzung des ISMS sind im Anhang des Bearbeitungsplans einige *mögliche* Hilfsmittel angegeben.

Die Geschäftsleitung der Sanamed hatte aufgrund des Audit-Berichts bereits grundsätzlich beschlossen, ein ISMS einzuführen. Die Art und Weise bzw. das weitere Vorgehen, insbesondere bezüglich der Ressourcen für die Umsetzung eines ISMS und der Einführung allenfalls notwendigen Sicherheitsmassnahmen, müssen noch beschlossen werden. Deshalb sollen Sie am letzten Tag der Fallstudienbearbeitung die wesentlichen Punkte Ihres Konzepts, inkl. der in den nächsten drei Jahren zu budgetierenden Aufwände und Kosten als Vorschlag vor der Geschäftsleitung von Sanamed präsentieren und genehmigen lassen. (Die für die IT verantwortliche Führungsperson von Sanamed ist Mitglied der Geschäftsleitung.) Der durch ihr Beraterteam zu präsentierende Vorschlag soll sich am Ist-Zustand der Informationssicherheit der Sanamed, den vorhandenen Risiken aus mindestens zwei ausgewählten Geschäftsprozessen sowie den Vorgaben des Standards ISO/IEC 27001:2013 orientieren.

2.4 Konformität zum Standard ISO/IEC 27001:2013

Die Kapitel 4 bis 10 des Standards 27001:2013 sind impilizit in einen PDCA-Kreislauf eingebettet. Die Aufgaben der Fallstudienbearbeitung sind auf die Bearbeitung dieser Kapitel 4 bis 10 in einem ersten PDCA-Durchlauf ausgerichtet. Gemäss der dem Standard zugrundeliegenden Idee sollen sich die Management-Teilprozesse, die sich aus den Unterkapiteln und

ihren Klauseln ergeben, sowie deren sicherheitsrelevanten Ergebnisse, bei jedem weiteren (zukünftigen) PDCA-Durchlauf verbessern können.

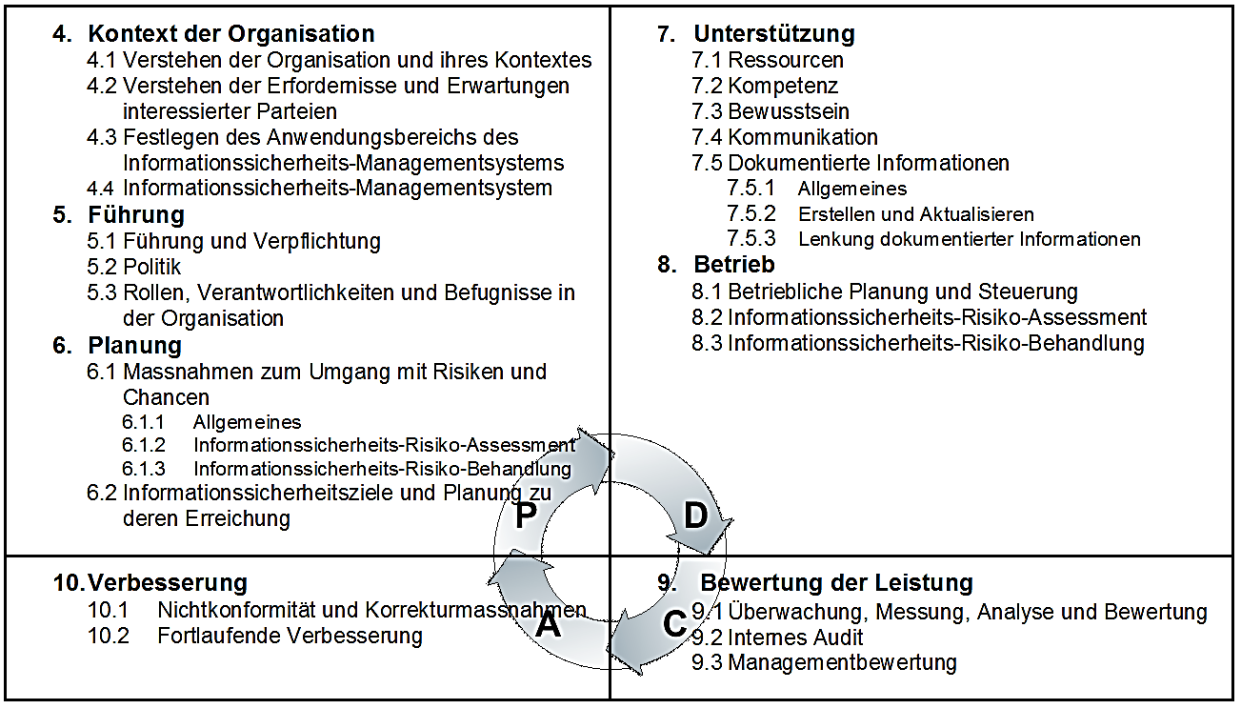


Abbildung 1: Aufbau von ISO/IEC 27001:2013 in einem impliziten PDCA-Zyklus

2.5 Erwartete Ergebnisse

Das in der Gruppe zu erstellende Einführungskonzept soll als managementgerechte Entscheidungsgrundlage für die Einführung eines ISMS nach ISO/IEC 27001:2013 dienen. Deshalb soll weniger auf die für eine Zertifizierung notwendige punktgenaue Erfüllung des Standards, sondern vielmehr auf die konzeptionelle Darstellung hinsichtlich der späteren Einführung des ISMS Wert gelegt werden.
Die minimal erwarteten Ergebnisse, die in das Einführungskonzept einfliessen sollen, sind als Lösungsmassstab der Aufgaben vorgegeben.
Der Sicherheitsprozess nach ISO/IEC 27001:2013 geht wie folgt in das Konzept ein:

Plan	**Festlegen Rahmenbedingungen für ISMS (Kontext der Organisation, Führung und Planung):** Zunächst werden die Unternehmens-Rahmenbedingungen und Sicherheitsgrundlagen (Kriterien, Methoden, Prozesse etc.) festgelegt, die für das Sicherheitsmanagement relevant sind. Dies erfolgt in der Regel top-down. Wichtige Anmerkung für die Konzepterstellung: Für die spätere Konkretisierung fliessen diese Rahmenbedingungen in das Einführungs-Konzept ein.
Do	**Umsetzen und Durchführen des ISMS (Unterstützung und Betrieb):** Die festgelegten Unternehmens-Rahmenbedingungen und Sicherheitsgrundlagen werden entsprechend umgesetzt und dokumentiert. Wichtige Anmerkung für die Konzepterstellung: Für die spätere Umsetzung des ISMS fliesst die Umsetzungsplanung der Prozesse des Managementsystems und wesentlichen Massnahmen in das Einführungs-Konzept ein.

Check	**Überprüfen des ISMS:** Die umgesetzten Massnahmen für den Betrieb des ISMS und für das Management der Informationssicherheits-Risiken werden anhand der definierten Vorgaben überwacht und überprüft und die Ergebnisse zur Kontrolle und Entscheidungsfindung an das Management berichtet. Wichtige Anmerkung für die Konzepterstellung: Für die spätere Umsetzung fliesst die Konzeption der entsprechenden Überwachungs- und Überprüfungsprozesse in das Einführungs-Konzept ein.
Act	**Verbessern des ISMS:** Basierend auf den Überwachungs- und Prüfungsergebnissen werden Verbesserungsmassnahmen abgeleitet, formuliert, eingeleitet und dokumentiert). Wichtige Anmerkung für die Konzepterstellung: Für die spätere Umsetzung fliesst die Konzeption der aus allfälligen Prüfungsergebnissen resultierenden Prozesse, Massnahmen und Aufgaben zur Verbesserung und Korrektur in das Einführungs-Konzept ein.

Die im Rahmen der Fallstudienbearbeitung benötigten detaillierten Unterlagen (Standard-Dokumente, Literatur, Hilfsmittel etc.) sind vorzugsweise im Konzept zu referenzieren (zitieren) und im Anhang zum Konzept aufzuführen.

2.6 Bewertungsgrundlagen

Die in der Gruppe erarbeiteten Lösungen werden weniger nach ihrer Richtigkeit bezüglich der Risikoeinschätzungen und der Massnahmenzuordnungen, als vielmehr nach dem Verständnis für die Einzelprozesse und der zugrundliegenden Idee des Standards (z.B. kontinuierliche Verbesserung, Einbezug des Managements und Nachvollziehbarkeit der Wirksamkeit) beurteilt.

Die Bewertung der Ergebnisse der Fallstudienbearbeitung durch die Dozenten erfolgt mit einem kurzen Bewertungsbericht pro Gruppe gemäss der im Studium bereits angewandten Bewertungsskala (s. Fallstudienbearbeitung Sanamed im CAS). Die Bewertungsberichte werden der Hochschule in der Regel innert zwei Wochen zugestellt.

Die Bewertung der erstellten Arbeiten (Konzept, Grundlagen, Hintergrundinformationen, Präsentation) beruht auf folgenden Punkten:

- Schriftliche Unterlagen (elektronisch): max. 30 Punkte

  Die abgegebenen Unterlagen werden gemäss den für Fallstudienbearbeitungen massgeblichen Bewertungsgrundlagen bewertet. Die Präsentation (schriftliche Version) ist ebenfalls abzugeben.

- Mündliche Präsentation: max. 5 Punkte

  Die Präsentation wird gemäss den für Fallstudienbearbeitungen massgeblichen Bewertungsgrundlagen bewertet.

- Individuelle Bewertung der Gruppenmitglieder: max. 5 Punkte
  Für eine entsprechend konstruktive Mitarbeit in der Gruppe während der gesamten Zeit.

Bei maximaler Leistung von Gruppe und Gruppenmitglied kann ein einzelnes Gruppenmitglied 40 Punkte, entsprechend der Note 6.0 erhalten.

3 Aufgabenstellungen

3.1 Aufgabenübersicht

Aufgabe 1: Erstellung eines *Vorgehensplans* für die Bearbeitung der Fallstudie und für die Erstellung eines ISMS-Einführungskonzepts

Aufgabe 2: „Kontext der Organisation“ und „Führung“ (plan)

Aufgabe 3: „Planung“ (plan)

Aufgabe 4: „Unterstützung“ und „Betrieb“ (do)

Aufgabe 5: „Bewertung der Leistung“ (check)

Aufgabe 6: „Verbesserung“ (act)

Aufgabe 7: Konsolidierung der Aufgabenergebnisse als Konzept in der Form eines Berichts an die Geschäftsleitung von Sanamed

Aufgabe 8: Erstellung und Durchführung einer Präsentation vor der Geschäftsleitung Sanamed

Generelles zu den Aufgaben:

- Die Details zu den Aufgaben entnehmen sie den folgenden Seiten. Die Muster in den Anhängen sind als allgemeine Beispiele zu verstehen; für den Fall Sanamed sind geeignete eigene Lösungen zu definieren oder mindestens die Inhalte anforderungsgerecht anzupassen. Allfällige Fragen werden durch anwesende Dozenten gerne beantwortet.
- Für eine ISMS-Einführung sind u.a. neben Funktionalität und Wirksamkeit, Zeitrahmen, Aufwand und Kosten der Massnahmen wichtig.
- Der Standard mit seinen einzelnen Klauseln wird vorteilhaft, wo möglich, mittels Einzel-Prozessen[3] im Rahmen eines PDCA-Zyklus behandelt, was die wichtige Voraussetzung für eine ständige Verbesserung des ISMS und seiner Resultate schafft.
- Denken Sie daran, dass die Ergebnisse aus den einzelnen Aufgaben in das Konzept einfliessen müssen und das Konzept am Schluss abgegeben sowie in zusammengefasster Form vor der fiktiven Geschäftsleitung präsentiert werden muss. Die detaillierten Ausarbeitungen (Word-Dokumente, Excel-Sheets, PowerPoint-Folien) müssen in konsolidierter Form als Anhang des Konzepts zur Bewertung abgegeben werden. Es ist notwendig, sich bereits zu Beginn sämtliche Aufgaben 1 - 8 durchzulesen, und einen Plan mit Zeitraster für die Erstellung des Konzepts zu erstellen.

[3] Bei der prozessorientierten Behandlung werden die Prozessvariablen wie Input, Hilfsmittel, Ziele, Owner, KPI (Key Performance Indicator), Frequenz und Output bestimmt.

3.2 Aufgabe 1: Erstellung eines *Vorgehensplans* für die Bearbeitung der Fallstudie und für die Erstellung eines ISMS-Einführungskonzepts

Ausgangslage und Input	• Szenario Fallstudie Sanamed • Unterlagen: - Grundlagen und Methoden Risikomanagement CAS IS CM 4.2; - Bestehende Standards u.a. ISMS (ISO/IEC 27001:2013), ISO/IEC 27002:2013 und ISO/IEC 27005:2011 sowie Anleitung in ISO/IEC 27003:2010; - Datenschutzgesetz und sonstige relevante Gesetzesanforderungen (s. Vorlesungen Recht); - Div. Rechtsgrundlagen im Zusammenhang Informationssicherheit und Datenschutz in Spitälern (s. beispielsweise „Merkblatt Datenschutz in den öffentlichen Spitälern des Kantons Solothurn“, Anhang 14).
Aufgabenbeschreibung	Es ist ein Vorgehensplan für die Bearbeitung der Fallstudie sowie für die Erstellung eines Konzepts für „Einführung und Betrieb eines ISMS auf der Basis ISO/IEC 27001:2013“ zu erstellen.
Lösungsmassstab zur Fallstudienbearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • die Idee des Standards, u.a. die Prozessorientierung als PDCA-Zyklus sowohl für die Einführung als auch für den Betrieb verstanden und veranschaulicht ist; • die Festlegungen getroffen sind, über welchen Bereich des Spitals oder über welche Geschäftsprozesse in einer ersten Phase das ISMS eingeführt werden soll (ein ISMS kann auch für ein sinnvolles Teilgebiet mit seinen Businessprozessen eingeführt werden. (s. ISO/IEC 27001:2013, Abschnitt 4.3); • ein grobes provisorisches Inhaltsverzeichnis des Konzepts erstellt ist; • ein grober Projektplan über die Einführung des ISMS; • die Aktivitäten der Gruppe zur Ausarbeitung der gestellten Fallstudien-Aufgaben[4] und zur Erstellung des Konzepts im Zeitraster dargestellt sind. (Zu den Aktivitäten gehören beispielsweise auch Recherchen über Anforderungen aus sozialen, rechtlichen, organisatorischen und technologischen Aspekten sowie für Spitäler bereits existierende Lösungen).
Bemerkung	Diese erste Aufgabe zwingt Sie, bereits zu Beginn der Fallstudienbearbeitung sich mit den weiteren gestellten Aufgaben (2 bis 8) der Fallstudienbearbeitung grob vertraut zu machen.

[4] Die Lösungen der einzelnen Aufgaben liefern wichtige Inhalte für das Einführungskonzept, da sie u.a. den PDCA-Zyklus des Standards bei den Einführungsaktivitäten widerspiegeln.

3.3 Aufgabe 2: „Kontext der Organisation“ und „Führung“

Ausgangslage und Input	• Szenario Fallstudie Sanamed • Informationssicherheitspolitik Sanamed • Output und Ergebnisse aus Aufgabe 1 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Erarbeiten Sie für Sanamed die folgenden 27001-Klauseln: 4.1 Verstehen der Organisation und ihres Kontextes 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien 4.3 Festlegen des Anwendungsbereichs des Informationssicherheits-Managementsystems 4.4 Informationssicherheits-Managementsystem 5.1 Führung und Verpflichtung 5.2 Politik 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • externe und interne Anliegen, die ein ISMS nahelegen, kurz aufgeführt sind; • die interessierten Kreise und deren Anforderungen erwähnt sind; • das Einsatzgebiet des ISMS für Sanamed definiert und dokumentiert ist (s. auch Aufgabe 1); • Beispiele von vorhandenen oder noch zu erreichenden Bekenntnissen zu Verpflichtungen von massgeblichen Führungspersonen zur Informationssicherheit und zu einem ISMS angeführt sind; • Inhaltspunkte der „Informationssicherheitspolitik[5]“ für das gesamte Spital in den wesentlichen Punkten (u.a. den gesetzlichen Anforderungen, die für Sanamed von besonderer Relevanz sind) stichwortartig definiert ist (Muster s. Anhang 2); • in welcher auch die für das ISMS bestimmten organisatorischen Rollen, Verantwortlichkeiten und Befugnisse festgelegt und aufgeführt sind.
Bemerkung	Sämtliche Aufgaben der Fallstudie müssen so bearbeitet werden, dass eine ständige Verbesserung des ISMS gemäss Aufgabe 6 möglich ist[6]. Die Muster in den Anhängen sind lediglich als allgemeine Beispiele zu verstehen.

[5] Informationssicherheitspolitik kann mit ISMS-spezifischen Politikinhalten ergänzt werden.

[6] Die ständige Verbesserung kann beispielsweise erreicht werden, indem einzelne Klauseln des Standards als Prozesse (Teilprozesse) behandelt werden, mit den Prozessvariablen Input, Output, Prozessziele, Key Performance Indikatoren (KPI) und Prozess-Owner.

3.4 Aufgabe 3: „Planung“

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Ergebnisse aus Aufgabe 2 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Analysieren Sie und definieren Sie die Teilprozesse für: 6.1 Massnahmen zum Umgang mit Risiken und Chancen 6.1.1 Allgemeines 6.1.2 Informationssicherheits-Risiko-Assessment 6.1.3 Informationssicherheits-Risiko-Behandlung 6.2 Informationssicherheitsziele und Planung zu deren Erreichung
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • ein Ansatz für ein geeignetes **Risiko-Assessment** einschliesslich der Kriterien für die Risiko-Akzeptanz definiert sind (s. Prozessablauf, Anhang 3 und Muster für semiquantitative Risikoeinstufung, s. Anhang 4); • wenigstens 10 Risiken des Falls identifiziert, analysiert und gemäss der erarbeiteten Einstufungskriterien analysiert und bewertet sind (s. Anhang 5: Asset Register für identifizierte Risiken und Anhang 6: Muster einer Tabelle für bewertete Risiken); • die **Risikobehandlung** gemäss dem Standard ISO/IEC 27001:2013 definiert und angewendet wird (s. Prozessablauf, Anhang 7); • die Controls (Massnahmen) in geeigneter Weise den Risiken zugeordnet sind (s. Muster, Anhang 8); • das Statement of Applicability (Anwendungsnachweis basierend auf Annex A des Standards) erstellt ist (s. Muster, Anhang 9); • ein Risiko-Behandlungsplan (s. Muster, Anhang 10) erstellt ist, in dem die Massnahmen und zu erwartenden Restrisiken in einer für das „Risk owner’s approval“ geeigneten Form zusammengestellt sind; • eine geeignetes Vorgehen für die Bewilligung der Restrisiken, Massnahmen-Definitionen und -Umsetzungen beispielhaft konzipiert und beschrieben ist (s. Muster, Anhang 11).
Bemerkung	Bereits in der Planphase sind die Teilprozesse für das Risiko-Assessment und die Risiko-Behandlung zu entwickeln und an konkreten Risiken (min. 10) zu demonstrieren. Die Muster in den Anhängen sind als allgemeine Beispiele zu verstehen.

3.5 Aufgabe 4: „Unterstützung“ und „Betrieb“

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Ergebnisse aus Aufgabe 3 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Konzipieren Sie die für die Umsetzung im Standard geforderten Unterstützungsanforderungen sowie die betriebliche Planung und Durchführung der Prozesse gemäss der folgenden Standard-Unterkapiteln aus ISO/IEC 27001:2013: 7.1 Ressourcen 7.2 Kompetenz 7.3 Bewusstsein 7.4 Kommunikation 7.5 Dokumentierte Informationen 7.5.1 Allgemeines 7.5.2 Erstellen und Aktualisieren 7.5.3 Lenkung dokumentierter Informationen 8.1 Betriebliche Planung und Steuerung 8.2 Informationssicherheits-Risiko-Assessment 8.3 Informationssicherheits-Risiko-Behandlung
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • eine Zusammenstellung der für ein funktionstüchtiges ISMS von Sanamed notwendigen Ressourcen und Kompetenz vorliegt; • eine Konzeption vorliegt, wie der funktionstüchtige Betrieb des ISMS und das Bewusstsein für die Informationssicherheit und gefördert werden kann; • ein Trainings- und Awareneskonzept vorgeschlagen ist (s. Beispiel, Anhang 12); • Verfahren für die Erkennung und Bewältigung von „Security Events“ und „Security Incidents“ vorgeschlagen sind; • ein Vorschlag vorliegt, wie und was im Zusammenhang mit der Informationssicherheit und dem ISMS kommuniziert wird; • ein Vorgehen vorliegt, wie die Teilprozesse für das Assessment (s. Risk Register, Anhang 6) und die Bewältigung (s. Behandlungsplan, Anhang 10) periodisch und bei signifikanten Veränderungen durchgeführt wird.
Bemerkung	-

3.6 Aufgabe 5: „Bewertung der Leistung“

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Ergebnisse aus Aufgabe 4 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Konzipieren Sie die Prozesse zur Überwachung und Überprüfung hinsichtlich nachhaltiger Sicherheit und ständiger Verbesserung des ISMS gemäss den 27001- Unterkapiteln: 9.1 Überwachung, Messung, Analyse und Bewertung 9.2 Internes Audit 9.3 Managementbewertung
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • Vorschläge für Vorgehen und Methoden erarbeitet sind, wie die Funktionstüchtigkeit des ISMS und dessen Prozesse und Massnahmen gemessen, analysiert und beurteilt werden können; • Vorschläge erarbeitet sind, wie das Interne Audit durchzuführen ist; • Vorschläge für die Berichterstattung unter Berücksichtigung der Findings und den Einbezug des Managements erarbeitet sind (s. Beispiel Anhang 13).
Bemerkung	-

3.7 Aufgabe 6: „Verbesserung“

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Ergebnisse aus Aufgabe 5 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Konzipieren Sie die Prozesse zur Gewährleistung der Verbesserungen und Korrekturen gemäss den 27001-Unterkapiteln: 10.1 Nichtkonformität und Korrekturmassnahmen 10.2 Fortlaufende Verbesserung
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • in groben Zügen ein Verfahren zur Berücksichtigung von Verbesserungen vorgeschlagen ist, welches nicht nur Nicht-konformitäten und Lücken in der Einhaltung des Standards korrigiert, sondern in wirksamer Weise sowohl heutige Sicherheitsmängel und Schadensereignisse behebt, als auch den zukünftigen Bedrohungen und Anforderungen mit entsprechenden Management-Handlungen gerecht werden kann; • ein Dokumentationsvorgehen in groben Zügen definiert ist, mit dem die Verbesserungen im Einzelnen nachgewiesen werden.
Bemerkung	-

3.8 Aufgabe 7: Konsolidierung der Aufgabenergebnisse als Konzept in der Form eines Berichts an die Geschäftsleitung von Sanamed

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Ergebnisse aus Aufgaben 1-6
Aufgaben-beschreibung	Konsolidierung der Teilergebnisse aus Aufgabe 1 bis 6, auf denen das ISMS aufgebaut werden kann, als Konzept in der Form eines Berichts an die Geschäftsleitung.
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • die Inhalte / Ergebnisse der einzelnen Aufgaben gut dokumentiert und als Konzept für den Aufbau eines ISMS konsolidiert sind; • die im Rahmen der Fallstudienbearbeitung erarbeiteten relevanten Grundlagen und Unterlagen in einem Anhang zum Konzept aufgeführt sind; • die im Konzept verwendeten und relevanten Unterlagen (Literatur, Standards etc.) richtig zitiert und referenziert sind; • das Konzept als wichtiges „Deliverable“ für den ISO von Sanamed ausgearbeitet ist, mit dem u.a. das ISMS-Projekt gesteuert und überwacht werden kann; • das Konzept als Soll-Vorgabe für allfällige Compliance-Überprüfungen herangezogen werden kann (z.B. Compliance zu gesetzlichen Anforderungen).
Bemerkungen	• Das Konzept einschliesslich der erarbeiteten Unterlagen werden benotet. In die Benotung geht u.a. auch die Übersichtlichkeit und Klarheit der Darstellung ein. • Die Kriterien für die Bewertung des Konzepts erfolgt gemäss dem aus der Fallstudienbewertung des CAS bereit bekannten Bewertungsschema.

3.9 Aufgabe 8: Erstellung und Durchführung einer Präsentation vor der Geschäftsleitung Sanamed

Ausgangslage	• Szenario Fallstudie Sanamed • Output und Konzept aus Aufgabe 7 • Unterlagen zu/aus Aufgabe 1
Aufgaben-beschreibung	Präsentation der wichtigsten Aussagen aus dem Konzept hinsichtlich Einführung und Betrieb des ISMS vor der fiktiven Geschäftsleitung (einschl. dem für die IT verantwortlichen Geschäftsleitungsmitglied) von Sanamed.
Lösungsmassstab zur Fallstudien-bearbeitung	Der minimale Lösungsumfang ist erreicht, wenn … • die Präsentation mit den wichtigsten Aussagen in nachvollziehbarer Weise dokumentiert ist (z.B. in Form eines PowerPoint-Files); • eine gute Präsentation vor der fiktiven Geschäftsleitung der Sanamed durchgeführt wurde (der IT-Verantwortliche ist GL-Mitglied).
Bemerkung	Die Bewertung der Präsentation erfolgt gemäss dem aus der Fallstudienbewertung des CAS bereits bekannten Präsentations-Bewertungsschema (s. Anhang 15) .

4 Anhänge

4.1 Anhang 1: Zusammenstellung Business-Prozesse aus früheren Analysen

- Patientenadministration (Führen von Patientenakten)
- Pflege
- Apotheke / Medikation
- Notfälle
- Hotellerie / Verpflegung
- Röntgen / Radiologie
- Operation
- Spitalpersonal / HR
- Labor
- Datenverarbeitungsprozesse / Informatikprozesse
- Gebäudeinfrastruktur/Technik / Sicherheit

4.2 Anhang 2: Gerüst für eine beispielhafte Informationssicherheitspolitik

- ❒ Geschäfte des Unternehmens und Rolle der Informationen und der IT
- ❒ Umwelt u.a. für Unternehmen wichtige Märkte und Technologien
- ❒ Wichtige Unternehmens-Assets, Geographische und örtliche Charakteristiken, Hauptsächliche Bedrohungen, Anspruchsgruppen und deren Sicherheitsbedürfnisse, Anforderungen gesetzlicher, regulatorischer und vertraglicher Art
- ❒ Für Informations-Sicherheit relevante Ziele und Grundsätze aus Unternehmens-Risiko-Politik und Kommitment des Managements bezüglich Einhaltung der Anforderungen , Ziele und Grundsätze
- ❒ Hinweis auf Risiko- und Sicherheitskultur, -bewusstsein, -kommunikation und Schulung
- ❒ Hinweis auf Mass der angestrebten „Unternehmens-Sicherheitsreife“ (bezogen auf angewandtes Maturity-Modell)
- ❒ Begriffsdefinition Informationen, IT-Systeme und deren Komponenten
- ❒ Einsatzbereich und Abgrenzung (Assets, Umfang) der Informationssicherheit und des ISMS
    - Informationen, IT-Systeme, IT-Prozesse über den gesamten Lebenszyklus, IT-Benutzer
    - Nicht zur Informations-Sicherheit gehörende Funktionen (z.B. physische Objekt-Sicherheit)
- ❒ Sicherheits- und Risikoziele und generelle Aussagen über deren Einhaltung
    - Vertraulichkeit (Datenschutz, Bankkundengeheimnis, Geschäfts-Geheimnis)
    - Integrität
    - Verfügbarkeit
    - Allenfalls auch Authentizität, Non-Repudiation, Zuverlässigkeit und Nachvollziehbarkeit
- ❒ Risiko-Management
    - Unternehmens-Risikomanagementprozess
    - Kriterien zur Risikoeinschätzung und Risikoakzeptanz
    - Methode und Hinweise auf Prozess-Beschreibungen
- ❒ Referenzieren der Prozesse für Geschäftskontinuität und IT-Notfall-Planung hinsichtlich Informationssicherheit
- ❒ Referenzieren der Informationssicherheits-Vorschriften (ggf. im Rahmen von SLAs)
    - für Outsourcing
    - für Externe und Vertragspartner
- ❒ Bereitstellung der erforderlichen Mittel und Ressourcen
- ❒ Bezugnahme auf weitere Weisungen über einzelne Risiko-Bereiche
- ❒ Festlegung der Verantwortlichkeiten und Kompetenzen:
    - Leiter von Geschäftseinheiten, / Organisationseinheiten
    - Mitarbeitende
    - CISO, CIO, IT-Prozess- und IT-System-Owner, Internes Audit
- ❒ Politik-Geltungsbereich: Z.B. Mitarbeitende des ganzes Unternehmen
- ❒ Inkraftsetzung: Datum Unterschrift CEO

4.3 Anhang 3: Teilprozesse Risiko-Assessment im Standard ISO/IEC 27001:2013

Informationssicherheits-Assessment-Prozess	
definieren und anwenden in Phase „plan“	**durchführen, periodisch oder bei signifikanten Veränderungen in Phase „do“**
a) etabliert und unterhält Informationssicherheits-Kriterien über 1) Akzeptanz-Kriterien und 2) Kriterien für die Durchführung eines Assessments	
b) garantiert, dass wiederholte Assessments zu konsistenten, gültigen und vergleichbaren Resultaten führen.	
c) identifiziert die Informationssicherheits-Risiken, 1) hinsichtlich Verlusten von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen 2) und Risiko-Owner ermittelt und benannt werden.	
d) analysiert die Informationssicherheits-Risiken, durch 1) Beurteilung der potentiellen Konsequenzen 2) Beurteilung die realistische Wahrscheinlichkeit (Häufigkeit) des Auftretens 3) Bestimmung der Risikohöhe	
e) bewertet die Informationssicherheits-Risiken, durch 1) Vergleich der Ergebnisse der Risikoanalyse mit etablierten Risikokriterien 2) Priorisierung der Risiken hinsichtlich ihrer Behandlung	
dokumentiert und archiviert die Informationen über den Risiko-Assessment-Prozess.	

4.4 Anhang 4: Risiko-Analyse

4.4.1 Risiko-Matrix zur Semiquantitative Einstufung

Monetarisierte Risiko-Werte in Mio. CHF					
bis 0.1	0.1 - 0.3	0.3 - 1	1 - 3	3 - 10	über 10
sehr klein	klein	mittel	gross	sehr gross	katastrophal

Schadenshöhe pro Fall **Häufigkeit der Fälle**	**E** klein	**D** mittel	**C** gross	**B** sehr gross	**A** katastro-phal
sehr oft (mehrmals pro Jahr)	mittel	gross	sehr gross	irreal	irreal
oft (1 mal in 1 – 3 Jahren)	klein	mittel	gross	sehr gross	irreal
selten (1 mal in 3 – 10 Jahren)	sehr klein	klein	mittel	gross	katastro-phal
sehr selten (1 mal in 10 – 30 Jahren)	sehr klein	klein	klein	mittel	katastro-phal
unwahrscheinlich (1 mal in mehr als 30 Jahren)	sehr klein	sehr klein	klein	mittel	katastro-phal (*)

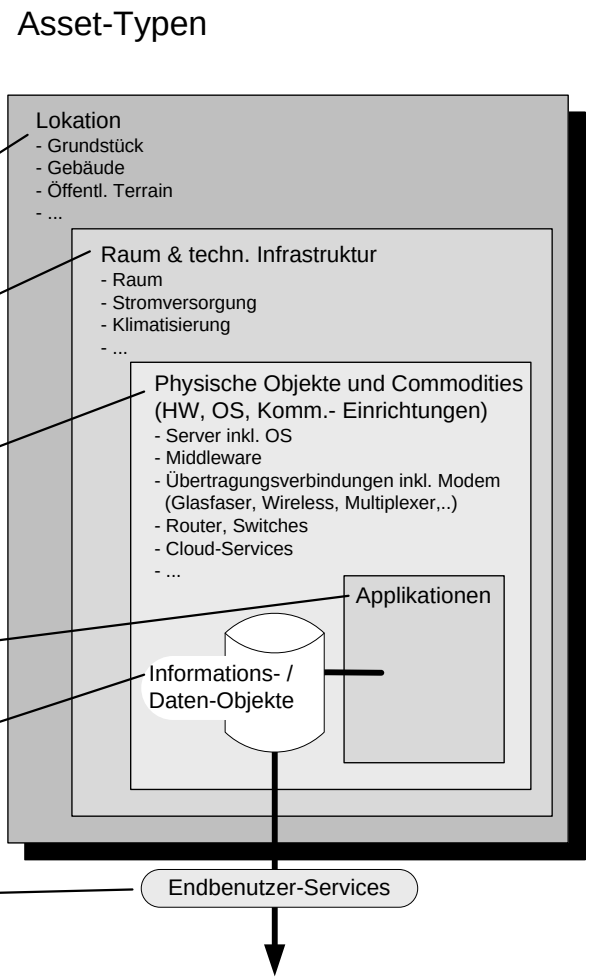
4.4.2 Schadens-Metrik zur Semiquantitative Einstufung (Beispiel)

Impact-Typen **Einstufung**	**Direkter finanzieller Verlust [CHF]** (Barwert der Ersatzkosten + Opportunitäts-Kosten)	**Sonstige firmentypische Schadensauswirkungen**		
		Schädigung der geschäftlichen und wirtschaftlichen Interessen Beeinträchtigung der Geschäfts- und Management-Vorgänge Verlust an Reputation und Goodwill	Nichteinhaltung gesetzlicher und regulativer Verpflichtungen (*)	Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen
		Beispiele		
A **katastrophal**	über 10 Mio. CHF (z.B. Verlust einer wichtigen Lizenz, so dass Geschäftstätigkeit aufgegeben werden muss)	Grossabnehmer künden Verträge aufgrund bekannt gewordener negativer Produkteeigenschaften (z.B. krebseregendes Nahrungsmittel)	-	Systematische Schädigung von Leib und Leben anderer Personen
B **sehr gross**	3 - 10 Mio. CHF (z.B. aufgrund lang anhaltender Produktionsausfälle)	Einige Abnehmer stellen auf Alternativprodukte um aufgrund abgeflossener Produktionsgeheimnisse oder irreparabler Imageschäden	Strafe infolge Verstoss gegen Kartellrecht	Schädigung von Leib und Leben anderer Personen im Einzelfall
C **gross**	1 - 3 Mio. CHF (z.B. aufgrund Zerstörung von Produktionssystemen und entsprechenden Produktionsausfällen)	Abnehmer drücken Preise aufgrund von durchgesickerten Geschäftsgeheimnissen	Sanktionen wegen grober Sorgfaltspflichtverletzung	Klage und Schadensersatz wegen Verletzung des Geschäftsgeheimisses der Abnehmer
D **mittel**	0.3 - 1 Mio. CHF (z.B. aufgrund Schadensersatzforderungen bei falschen Lieferungen)	Erhöhte Werbeanstrengungen nötig, infolge angeschlagener Reputation	Verfahren wegen Mängel in der ordnungsgemässen Geschäftsführung	Klagen wegen indiskreter Behandlung von Personaldaten
E **klein**	bis 0.3 Mio. CHF (z.B. aufgrund kleinerer Störungen und daraus entstandener Ausschussteile)	-	-	Schadensersatz wegen vereinzelter Verletzung des Datenschutzes

* z.T. persönliche Haftung verantwortlicher leitender Personen

4.5 Anhang 5: Asset Register (Beispiel)

	Nr.	Asset-Bezeichnung	Ort	Owner
Unterstützende Assets	8	Personal		
	8.1			
	8.2			
	…			
	7	Organisation		
	7.1			
	7.2			
	…			
	6	Lokationen		
	6.1			
	6.2			
	…			
	5	Räume und technische Infrastruktur		
	5.1			
	5.2			
	…			
	4	Physische Objekte und „Commodities“ (Hardware, Betriebs- und Kommunikationssysteme etc.)		
	4.1			
	4.2			
	…			
	3	Applikationen		
	3.1			
	3.2			
	…			
Primäre Assets	2	Informations- und Datenobjekte		
	2.1			
	2.2			
	…			
	1	Endbenutzer-Services		
	1.1			
	1.2			
	…			



4.6 Anhang 6: Analysierte und bewertete Risiken im Risk Register (Beispiel)

Risiko-Assessment															
Identifikation							Analyse							Bewertung	
Nr.	Primärer Asset	Unterstützende Assets	Risikobezeichnung	Spezifische Bedrohung	Schwachstellen (& Abhängigkeiten	Schadensszenario	Schaden s. klein (1) klein (2) mittel (3) gross (4) s. gross(5)			Informations- Kriterium			Häufigkeit > 5 Mal pro Jahr (5) 1-5 Mal pro Jahr (4) 1 Mal in 1-3 Jahre (3) 1 Mal 3-10 Jahre (2) 1 Mal >10 Jahre (1)	Akzeptanz-Vorgaben: a = vermeiden oder reduzieren; b= bewältigen nach wirtschftl. Aspekten c = tragen unter Beobachtung. Zeitprioritäten für Umsetzung: 1 = hoch: sofort; 2 = mittel: im Rahmen Budget; 3 = tief: in nächster Strategie- / Budget-Periode einplanen.
							Wiederherstellungskosten	Imageverlust	Direkter finanzieller Schaden	Verfügbarkeitsverlust	Vertraulichkeitsverlust	Integritätsverlust		
1.1	Zahlungsverkehr E-Banking	Hardware Software Personal	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke		4	3		x	x	3	a1
1.2		Authentisierungs-system Hardware Software	Ausspähen Bankdaten		Schwaches Authentisierungs-verfahren			4	3		x	x	2	a2
1.3		Internet Portal Netzwerk Hardware Sicherheitssoftware	Lahmlegen E-Banking	Denial of Service-Attacke	keine technischen und vorsorglichen Massnahmen	gezielte Blockade des Internet-Zugangs mittels Distributed-Denial-of-Service-Attacke	2	3	3	x			2	b3
....	....	.....	....	.....	.....	....	...	...	...	...	...	...	....	.....

Risiko-Bewertung der „Wichtigkeit“ der Massnahmen anhand Risiko-Matrix mit farblich gekennzeichneten Akzeptanzvorgaben:

Häufigkeit						
	4	b	b	a	a	a
	3	b	b	b	a	a
	2	c	b	b	b	a
	1	c	c	b	b	b
	0	c	c	c	b	b
		0	1	2	3	4
		Schaden				

Risiko-Bewertung sowohl nach „Wichtigkeit“ als auch nach „Dringlichkeit“ der Massnahmen

4.7 Anhang 7: Teilprozesse Risikobehandlung im Standard ISO/IEC 27001:2013

Informationssicherheits-Treatment-Prozess	
definieren und anwenden in Phase „plan“	**durchführen, periodisch oder bei signifikanten Veränderungen in Phase „do“**
a) den Ergebnissen des Risiko-Assessments angemessene Behandlungsoptionen selektieren.	
b) sämtliche Massnahmen um die Behandlungsoptionen umsetzen.	
c) die bestimmten Massnahmen mit den Massnahmen in Annex A vergleichen, um festzustellen, dass keine notwendige Massnahme ausgelassen wurde.	
d) ein Statement of Applicability erstellen, das alle notwendigen Massnahmen enthält einschliesslich der Begründungen für deren Verwendung und ob sie bereits implementiert sind sowie die Begründungen für die Auslassungen.	
e) ein Informationssicherheit-Risiko Behandlungsplan formulieren.	
f) die Einwilligung des Risiko-Owners zum Risikobehandlungsplan und der Akzeptanz von Restrisiken erlangen.	
Informationen über den Risiko-Behandlungs-Prozess dokumentieren und archivieren.	

4.8 Anhang 8: Massnahmenzuordnung im Risk Register (Beispiel)

Risiko-Assessment																Risiko-Behandlung	
Identifikation							Analyse							Bewertung	Massnahmen		
Nr.	Primärer Asset	Unterstützende Assets	Risikobezeichnung	Spezifische Bedrohung	Schwachstellen (& Abhängigkeiten	Schadensszenario	Schaden: Wiederherstellungskosten	Schaden: Imageverlust	Schaden: Direkter finanzieller Schaden	Informations- Kriterium: Verfügbarkeitsverlust	Informations- Kriterium: Vertraulichkeitsverlust	Informations- Kriterium: Integritätsverlust	Häufigkeit	Akzeptanz-Vorgaben: a = vermeiden oder reduzieren; b= bewältigen nach wirtschftl. Aspekten c = tragen unter Beobachtung. Zeitprioritäten für Umsetzung: 1 = hoch: sofort; 2 = mittel: im Rahmen Budget; 3 = tief: in nächster Strategie- / Budget-Periode einplanen. Restrisiko nach Massnahmen in Klammer	v=vermeiden, r=reduzieren, t=transfeieren, b=bewusst unter Beobachtung tragen	Massnahmen (einschl. bereits vorhandene Massnahmen) / Bemerkungen
							s. klein (1) klein (2) mittel (3) gross (4) s. gross(5)						> 5 Mal pro Jahr (5) 1-5 Mal pro Jahr (4) 1 Mal in 1-3 Jahre (3) 1 Mal 3-10 Jahre (2) 1 Mal >10 Jahre (1)			
1.1	Zahlungsverkehr E-Banking	Hardware Software Personal	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke		4 (3)	3 (3)		x	x	3 (2)	a1 (c)	r	• Brief an Kunden über Vorsichtsmassnahmen bei der Benutzung E-Banking, A.7.2.2 • Restrisiko wird bewusst unter Beobachtung tragen
1.2		Authentisierungs-system Hardware Software	Ausspähen Bankdaten		Schwaches Authentisierungs-verfahren			4 (2)	3 (2)		x	x	2 (2)	a2 (c)	r	• Starkes Authentifizier-Verfahren, 9.4.2 • Restrisiko wird bewusst unter Beobachtung
1.3		Internet Portal Netzwerk Hardware Sicherheitssoftware	Lahmlegen E-Banking	Denial of Service-Attacke	keine technischen und vorsorglichen Massnahmen	gezielte Blockade des Internet-Zugangs mittels Distributed-Denial-of-Service-Attacke	2 (1)	3 (2)	3 (2)	x			2 (2)	b3 (c)	r	• Abwehrsystem Telekom einrichten, 13.1.2 • Vorgehen im Rahmen BCM planen, 17.1.1, 17.1.2 • Restrisiko wird bewusst unter Beobachtung tragen
....	....	.....	....	.....	.....	....	...	...	...	...	...	...	....	.....	....	.....

4.9 Anhang 9: Statement of Applicability (Beispiel)

Paragraph	Massnahmenziel (Control Objective 27002)	Massnahme (Control 27002)	Anwendbar ja/nein	Bemerkungen: 1) Begründung Massnahmenwahl 2) Bereits bestehende Massnahmen 3) Nichtverwendung von Massnahmen aus Anhang A und Begründung 4) Referenz-Dokumente (Beispiele)
Anhang A				
A.5	**Information security policies**			
A.5.1	Management direction for information security	A.5.1.1 Policies for information security	ja	Dokumente Nr. 001 „Informationssicherheits- Politik“ Nr. 002 bis Nr. 013 „Information security policies“ für spezifische Sicherheitsgebiete (Policies =Weisungen, Richtlinien, Standards etc.)
		A.5.1.2 Review of policies for information security	ja	Vorgehen (Prozess, Frequenz, Adressaten etc.) in Dokument 001 festgelegt.
A.6	**Organisation of information security**			
A.6.1	Internal Organisation	A.6.1.1 Information security roles and responsibilities	ja	In Dokument Nr. 001 „Informationssicherheits- Politik“ festgelegt.
		A.6.1.2 Segregation of duties	ja	Zuständigkeitsmatrix Dokument Nr. 014
...	...	...	...	...

4.10 Anhang 10: Behandlungsplan (Beispiel)

Risiko-Assessment							Risiko-Behandlung		Massnahmen-Umsetzung				
Identifikation						Bewertung	Massnahmen						
Nr.	Primärer Asset	Unterstützende Assets	Risikobezeichnung	Spezifische Bedrohung	Schwachstellen (& Abhängigkeiten)	**Akzeptanz-Vorgaben:** a = vermeiden oder reduzieren; b= bewältigen nach wirtschftl. Aspekten c = tragen unter Beobachtung. **Zeitprioritäten für Umsetzung:** 1 = hoch: sofort; 2 = mittel: im Rahmen Budget; 3 = tief: in nächster Strategie- / Budget-Periode einplanen. Restrisiko nach Massnahmen in Klammer	v=vermeiden, r=reduzieren, t=transfeieren, b=bewusst unter Beobachtung tragen	Massnahmen (einschl. bereits vorhandene Massnahmen) / Bemerkungen	Massnahmenumsetzung gemäss Akzeptanzvorgaben Umsetzungsmethoden und bereits umgesetzte Massnahmen siehe SoA	Termin	Ressourcen / Budget	verantwortlicher Owner	Status
1.1	Zahlungsverkehr E-Banking	Hardware Software Personal	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	a1 (c)	r	• Brief an Kunden über Vorsichtsmassnahmen bei der Benutzung E-Banking, A.7.2.2 • Restrisiko wird bewusst unter Beobachtung tragen	1. Prio	30.03.2014	2 PT	HAS	offen
1.2		Authentisierungs-system Hardware Software	Ausspähen Bankdaten		Schwaches Authentisierungs-verfahren	a2 (c)	r	• Starkes Authentifizier-Verfahren, 9.4.2 • Restrisiko wird bewusst unter Beobachtung	2. Prio	30.06.2014	10 PT	LOS	offen
1.3		Internet Portal Netzwerk Hardware Sicherheitssoftware	Lahmlegen E-Banking	Denial of Service-Attacke	keine technischen und vorsorglichen Massnahmen	b3 (c)	r	• Abwehrsystem Telekom einrichten, 13.1.2 • Vorgehen im Rahmen BCM planen, 17.1.1, 17.1.2 • Restrisiko wird bewusst unter Beobachtung tragen	3. Prio	31.12.2014	3 PT	DOS	offen
….	….	…..	….	…..	…..	…..	….	……	…..	….	…..	…..	…..

4.11 Anhang 11: Management Kommitment mit Unterschriftentabelle (Beispiel)

…….

……..

…….

Stelle/Rolle	Name	genehmigt	Datum	Unterschrift
Applikations-/ Betriebs-Owner	J. Herrmann	genehmigt		.....
Entwicklungs-Owner	F. Beutler	genehmigt		.....
Netzwerk- und Plattform-Owner	J. Flach	genehmigt		.....
Security Officer IT-COFA	H. Meister	genehmigt		

4.12 Anhang 12: Muster Awareness-Plan

Lfd. Nr.	Aktion	Adressaten	Häufigkeit / Auslöser	Umfang / Dauer
1	Einführung in Informations-Sicherheit in Ordner für neueintretende interne MA	Neueintretende, interne Mitarbeitende	Arbeitsantritt	1/2 Std.
2	Einführung in Informations-Sicherheit für neueintretende externe MA	Externe Mitarbeitende	Arbeitsantritt	1/2 Std.
5	Informations-Sicherheits-Flyer	Alle internen und externen Mitarbeitenden	Abgabe bei sämtlichen Anlässen Informations-Sicherheit	4 Seiten
	…	….	….	…

4.13 Anhang 13: Checkliste für „management review“ (Beispiel)

4.13.1 Eingabe in Geschäftsleitungssitzung vom…….

Anforderungen		Bemerkungen /Dokumente	
a)	Ergebnisse der ISMS Audits und –Überprüfungen		❒
b)	Rückmeldungen von Interessenten		❒
c)	Techniken, Produkte oder Verfahren, die in der Organisation zur Verbesserung der Leistung und Wirksamkeit des ISMS eingesetzt werden können		❒
d)	Status von Korrekturmassnahmen und Vorbeugungsmassnahmen		❒
e)	Schwachstellen und Bedrohungen, die in der vorherigen Risikoeinschätzung nicht angemessen berücksichtigt wurden		❒
f)	Ergebnisse von Messungen der Wirksamkeit		❒
g)	Folgeaktivitäten nach vorherigen Managementbewertungen		❒
h)	Änderungen, die sich auf das ISMS auswirken könnten		❒
i)	Empfehlungen für Verbesserungen		❒

Datum: Unterschrift:

4.13.2 Ergebnisse in Stichworten aus Geschäftsleitungssitzung vom…….

Ergebnisse		Bemerkungen /Dokumente	
a)	Verbesserung der Wirksamkeit des ISMS		❒
b)	Aktualisierung der Risikoeinschätzungsplans und des Risikobehandlungsplans		❒
c)	Ggf. Änderungen an Verfahren und Massnahmen zum Erreichen von Informationssicherheit, um auf interne und externe Ereignis zu reagieren, die eine Auswirkung auf das ISMS haben könnten, einschliesslich Änderungen an:		❒
	1) Geschäftsanforderungen		❒
	2) Sicherheitsanforderungen		❒
	3) Geschäftsprozesse		❒
	4) Gesetzliche oder amtliche Anforderungen		❒
	5) Vertragliche Verpflichtungen		❒
	6) Risikoniveaus und/oder den Kriterien für Risikoakzeptanz		❒
d)	Bedarf an Ressourcen		❒
e)	Verbesserungen an der Art und Weise, wie die Wirksamkeit gemessen wird.		❒
f)	Ergebnisse von Messungen der Wirksamkeit		❒
g)	Folgeaktivitäten nach vorherigen Managementbewertungen		❒

4.14 Anhang 14: Merkblatt Datenschutz in den öffentlichen Spitälern des Kantons Solothurn

1. Ziele dieses Merkblattes

In der Solothurner Spitäler AG (soH)[1] sowie in Spitälern, mit denen der Kanton Solothurn einen Leistungsauftrag erteilt hat[2], werden Personendaten über Patientinnen und Patienten[3] vom Eintritt bis zum Austritt bearbeitet.[4]

Dieses Merkblatt will Patienten, das Spitalpersonal sowie die Aufsichtsbehörden informieren, wie die Daten von Patienten unter Einhaltung des Datenschutzes bearbeitet werden.

2. Allgemeine datenschutzrechtliche Grundsätze

In den öffentlichen Spitälern[5] müssen die allgemeinen datenschutzrechtlichen Grundsätze der Bearbeitung von Personendaten beachtet werden (§ 15 ff. des Informations- und Datenschutzgesetzes, InfoDG).[6]

Rechtsgrundlage: Vor allem sind dies das InfoDG, das kantonale Gesundheitsgesetz[7], das kantonale Spitalgesetz, eidgenössische Sozialversicherungsgesetze wie das Krankenversicherungsgesetz (KVG)[8], das Bundesgesetz über die Unfallversicherung (UVG)[9], das Bundesgesetz über die Invalidenversicherung (IVG)[10], das eidg. Datenschutzgesetz[11] (für private Haftpflichtversicherungen, private Lebensversicherungen etc.) oder die ausdrückliche Einwilligung des Patienten;

Zweckbindung: Daten über Patienten dürfen grundsätzlich nur zum Zweck, zu welchem sie vom öffentlichen Spital beschafft werden, z.B. zur Aufnahme, zur medizinischen Behandlung inklusive Operation, zur Pflege des Patienten, zur Rechnungstellung der Spitalleistungen, bearbeitet werden. Sollen Patientendaten

[1] Siehe kantonales Spitalgesetz (in Kraft seit 01.01.2006), das kantonale Spital hat folgende Standorte: Spital Solothurn - Grenchen, Kantonsspital Olten, Spital Dornach, Höhenklinik Allerheiligenberg, Psychiatrische Dienste des Kantons Solothurn.

[2] Spitäler mit einem Leistungsauftrag sind selbständige oder unselbständige Institutionen/Betriebe, welche öffentliche Aufgaben erfüllen und damit Behörden im Sinne des Informations- und Datenschutzgesetzes (InfoDG). Sie müssen deshalb die Bestimmungen des InfoDG ebenfalls beachten (§ 3 Bst. c InfoDG).

[3] Der Einfachheit halber wird im Folgenden die weibliche Form nicht angeführt.

[4] „Bearbeiten" ist jeder Umgang mit Daten, namentlich Erheben, Beschaffen, Aufzeichnen, Sammeln, Aufbewahren, Verwenden, Umarbeiten, Verändern, zugänglich Machen, Bekanntgeben, Veröffentlichen, Archivieren und vernichten (§ 6 Abs. 5 InfoDG).

[5] Im Folgenden sind unter „öffentlichen Spitälern" sowohl die soH als auch Spitäler mit Leistungsauftrag zu verstehen.

[6] BGS 114.1, weitere generelle Informationen zu den allgemeinen datenschutzrechtlichen Grundsätzen unter www.datenschutz.so.ch – Rechtsgrundlagen – Botschaft und Entwurf des Regierungsrates an den Kantonsrat

[7] BGS 811.11

[8] SR 832.10

[9] SR 832.20

[10] SR 831.20

[11] SR 235.1

für andere Zwecke bearbeitet werden, braucht es eine Rechtsgrundlage (§ 16 Abs. 2 InfoDG);

- Verhältnismässigkeit: Das öffentliche Spital darf nur die Patientendaten bearbeiten, welche für die medizinische Behandlung, die Rechnungstellung geeignet und nötig sind. Das Spitalpersonal darf dabei auch nur auf diejenigen Patientendaten elektronisch zugreifen oder Einsicht in papierene Dossiers nehmen, soweit dies nötig ist. Nur wenn Dritte Patientendaten effektiv benötigen, dürfen sie auch an diese bekanntgegeben werden (§ 16 Abs. 1 Bst. a InfoDG) 12;

- Transparenz: Patienten müssen informiert sein, wer was mit ihren Daten im Spital macht (§ 16 Abs. 1 Bst. a InfoDG). Die Transparenz wird einerseits in den Rechtsgrundlagen aber auch mit diesem Merkblatt geschaffen. Im übrigen informieren die Spitäler alle eintretenden Patienten in geeigneter Weise über ihre Rechte und Pflichten als Patienten (§ 83 der kantonalen Vollzugsverordnung zum Gesundheitsgesetz)[13];

- Richtigkeit, Vollständigkeit, Aktualität: Die für den Datenschutz verantwortlichen Stellen müssen regelmässig kontrollieren, ob die Daten über die Patienten richtig, vollständig und aktuell sind. Der medizinische Behandlungsverlauf muss chronologisch aufgezeichnet und auf dem aktuellsten Stand sein (§ 16 Abs. 1 Bst. b InfoDG, § 20 Abs. 1 und 2 des kantonalen Gesundheitsgesetzes);

- Auskunfts- und Einsichtsrecht, andere Rechte gegen Datenschutzverletzungen: Das Recht des Patienten, jederzeit ohne Angabe von Gründen auf Verlangen Auskunft oder Einsicht in die über ihn im öffentlichen Spital bearbeiteten Daten zu erhalten, muss unbedingt gewährleistet sein (§ 26 ff. InfoDG[14]);

- Datensicherheit: Angemessene technische und organisatorische Massnahmen zum Schutz der im Spital aufbewahrten Patientendaten müssen getroffen worden sein. So dürfen etwa medizinische Daten nur verschlüsselt via E-Mail versendet werden (§ 16 Abs. 1 Bst. c InfoDG).[15]

3. Personendaten[16] in öffentlichen Spitälern

Folgende Personendaten über Patienten werden in öffentlichen Spitälern erfasst und bearbeitet:

- Administrative Daten (Stammdaten), wie z.B. Name, Vorname, Adresse des Patienten, Geburtsdatum, Nationalität, Geschlecht, Konfession/Religion;

12 Siehe Ziffer 8, S. 8 ff. dieses Merkblattes

13 BGS 811.12

14 Siehe Ziffer 7.5, S. 8 dieses Merkblattes und ganz allgemein das Merkblatt „Ihre Rechte nach dem Informations- und Datenschutzgesetz“, abrufbar unter www.datenschutz.so.ch – Merkblätter.

15 Für weitere Informationen zur Datensicherheit wird auf das Merkblatt der Vereinigung der Schweizerischen Datenschutzbeauftragten „Der sichere Umfang mit Informations- und Kommunikationsgeräten“ verwiesen, welches ebenfalls abrufbar ist unter www.datenschutz.so.ch – Merkblätter.

16 „Personendaten“ sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person (betroffene) Person beziehen (§ 6 Abs. 2 InfoDG). Dazu gehören auch Nummern oder Codes, welche einer bestimmten Person zugeordnet sind (Pseudonyme).

O Medizinische Daten (Falldaten), die Krankengeschichte = alle Behandlungsschritte vom Eintritt bis zum Austritt, z.B. Eintrittsdiagnose, Untersuchungen, Operationen, Operationsberichte, Medikamente, Labortests, Röntgenbilder, Pflege, Austrittsdiagnose, Spitalrechnung.

Das Spitalpersonal beschafft besonders schützenswerte Personendaten seiner Patienten. Im Vordergrund stehen dabei Angaben über deren Gesundheit (= medizinische Daten). 17 Aus Personendaten kann unter Umständen ein Persönlichkeitsprofil über jeden Patienten erstellt werden, das Auskunft über dessen Gesundheit, Ansichten und Verhaltensweisen gibt.18

(Besonders schützenswerte) Personendaten über Patienten werden in der soH sowohl in elektronischer Form im Spitalinformationssystem hospis19 als auch in Papierform beschafft, aufbewahrt, weiterbearbeitet. Andere öffentliche Spitäler haben ihre eigenen Informationssysteme und bewahren die papierenen Dossiers auch selber auf.

4. Verantwortliche Stellen innerhalb des öffentlichen Spitals für den Datenschutz (Datenherr)

Nach aussen hin trägt für den Bürger das jeweilige öffentliche Spital letztendlich die Gesamtverantwortung für die Einhaltung des Datenschutzes. Innerhalb eines öffentlichen Spitals ist aber datenschutzrechtlich die Verantwortung aufgeteilt. Diejenige Stelle innerhalb des öffentlichen Spitals, welche den Patienten behandelt oder Patientendaten bearbeitet, ist auch verantwortlich für den Datenschutz. Dabei ist noch zu unterscheiden zwischen medizinischen und administrativen Patientendaten.

4.1 Für medizinische Personendaten

O Im ambulanten Bereich trägt der Chefarzt die Gesamtverantwortung. Der jeweilige behandelnde Arzt sowie das übrige Spitalpersonal (Hilfspersonal) sind ihrerseits verantwortlich, dass sie den Datenschutz der Patienten, welche sie behandeln, einhalten20;

O Im stationären Bereich liegt die Gesamtverantwortung beim Chefarzt der jeweiligen Klinik oder Abteilung. Der jeweilige behandelnde Arzt sowie das übrige Spitalpersonal sind für die Einhaltung des Datenschutzes ihrer Patienten verantwortlich.

O Sonderfall Belegärzte: Diese sind für die Bearbeitung von medizinischen Daten in ihrer eigenen Praxis selber verantwortlich.

[17] Im Laufe eines Spitalaufenthaltes können auch andere besonders schützenswerte Personendaten über den Patienten bearbeitet werden, wie z.B. über seine Konfession, wenn er den Besuch seines Pfarrers wünscht (§ 6 Abs. 3 InfoDG)

[18] § 6 Abs. 4 InfoDG

[19] Spitalinformationssystem hospis und Leistungserfassungs- bzw. Umsysteme (Vanadium, zentrale Bettendisposition, Radiologiesystem, Laborsystem), klinische Informationssysteme (Operationsberichte), siehe im Zentralen Register Datensammlungen, einsehbar bei der Staatskanzlei, den Oberämtern und beim kantonalen Beauftragten für Information und Datenschutz (IDSB), hospis wurde vom IDSB geprüft und für datenschutzrechtlich zulässig befunden.

[20] Arztsekretärinnen, Pflegepersonal, spitaleigenes Apotheke- und Laborpersonal, Finanz- / Rechnungs-wesen sowie die übrige allgemeine Spitalverwaltung, Informatik-Abteilung, technisches Spitalpersonal, Codierabteilung.

4.2 Für administrative Daten

Die für die Patientenadministration und das Rechnungswesen zuständige Stelle des öffentlichen Spitals.

Beispiel Spitalrechnung: Die für das Rechnungswesen bzw. Patientenadministration zuständige Stelle erhält vom Arzt so viele medizinische Daten über die erfolgte Behandlung, dass sie die Rechnung erstellen und der Krankenkasse oder dem Patient zustellen kann. Hat der Patient nur medizinische Fragen, beantwortet diese der zuständige Chefarzt respektive das von diesem bestimmte medizinische Personal (z.B. behandelnder Arzt) und nicht z.B. ein Mitarbeiter der Patientenadministration. Antworten auf rein finanzielle Fragen im Zusammenhang mit der Spitalrechnung (z.B. Tarif) gibt hingegen die für das Rechnungswesen bzw. die Patientenadministration zuständige Stelle.

5. Aufbewahrung, Archivierung und Vernichtung von Patientendaten

Aufbewahrungsdauer medizinischer Patientendaten: Medizinische Personendaten sind 10 Jahre aufzubewahren. Diese Frist beginnt an dem Tag, an welchem das letzte Dokument abgelegt oder der letzte Eintrag gemacht wurde (§ 20 Abs. 3 des kantonalen Gesundheitsgesetzes). [21]

Ausnahmsweise kann im Einzelfall diese 10-jährige Frist auf den Zeitpunkt verlängert werden, in welchem die medizinischen Daten nicht mehr benötigt werden, z.B. bei Prozessen wegen ärztlichen Kunstfehlern bis 1 Monat nach rechtskräftigem Abschluss des Prozesses, § 19 Abs. 1 InfoDG.

Aufbewahrungsdauer administrativer Patientendaten: Für die administrativen Patientendaten wird ebenfalls eine Aufbewahrungspflicht von 10 Jahren empfohlen, die in Ausnahmefällen verlängert werden kann, weil diese eng mit den medizinischen Patientendaten verknüpft sind (§ 19 Abs. 1 InfoDG).[22]

Vernichtung nach Ablauf der Aufbewahrungsfrist: Patientendaten, bei welchen die Aufbewahrungsfrist abgelaufen ist, müssen grundsätzlich umgehend vernichtet werden (Schredder, an Kehrrichtverbrennungsanlage zur Verbrennung überführen, elektronische Daten endgültig löschen). Vorbehalten bleibt die kantonale Archivgesetzgebung.[23]

6. Schweigepflicht

Datenschutz der Patienten und Schweigepflicht der Ärzte, des Hilfspersonals, stehen sehr eng zueinander. Die Schweigepflicht (Patientengeheimnis bzw. Berufsgeheimnis nach § 18 des kantonalen Gesundheitsgesetzes, Amtsgeheimnis nach § 38 des

[21] Die 10-Jahresregelung im kantonalen Gesundheitsgesetz erweist sich für bestimmte medizinische Daten als zu kurz. So können im Rahmen einer Übergangslösung bis zu einer entsprechenden Gesetzesänderung gestützt auf § 15 Abs. 2 Bst. b InfoDG gewisse medizinische Personendaten auch länger aufbewahrt werden, sofern dies für die konkrete Aufgabenerfüllung unentbehrlich ist und den Interessen des Patienten entspricht (z.B. Röntgenbilder, Laborwerte).

[22] Für reine Finanzdaten wie Geschäftsbücher, Buchhaltungsbelege und die Geschäftskorrespondenz gilt die 10-jährige Aufbewahrungsfrist nach Art. 962 des Bundesgesetzes über das Obligationenrecht, OR, SR 220

[23] § 19 Abs. 2 InfoDG

kantonalen Staatspersonalgesetzes[24]) soll die Vertrauensbeziehung des Patienten zu seinem Arzt respektive dem übrigen Hilfspersonal schützen. Was der Patient dem Arzt, dem Pflegepersonal, „im Vertrauen sagt", soll nicht einfach an jedermann weitergesagt werden. Dasselbe gilt von Beobachtungen über Patienten.

Verletzungen des Patientengeheimnisses bzw. Berufsgeheimnisses und des Amtsgeheimnisses sind grundsätzlich strafbar (Art. 320 und 321 des Schweizerischen Strafgesetzbuches, StGB [25]) und können ebenso disziplinarrechtlich geahndet werden.

Beispiele von Patientendaten, welche unter das Patientengeheimnis bzw. das Berufsgeheimnis und das Amtsgeheimnis fallen:

- Karl Muster, Regierungsrat, ist wegen Krebs im Spital;
  - Anne Meier ist wegen Magenbeschwerden hospitalisiert, die bevorstehende Scheidung macht ihr schwer zu schaffen;
  - Die Krankenkasse von Willi Grimm bezahlt die Spitalrechnung einfach nicht, Willi Grimm ist erbost und teilt am Telefon wüste Schimpfwörter aus.

Das Spitalpersonal sollte solche Aussagen auch nicht „laut" auf dem Gang, bei offener Tür des Stationszimmers, in der Cafeteria, machen, weil immer jemand zuhören und diese Informationen weiterleiten könnte.

Das Spitalpersonal ist von der Schweigepflicht entbunden, wenn einer der folgenden Gründe gegeben ist:

- Bei ausdrücklicher Einwilligung des betroffenen Patienten im Einzelfall. Allgemeine Einwilligungen oder Einwilligungsklauseln in Verträgen oder Allgemeinen Geschäftsbedingungen, z.B. „ich entbinde das Spital X von der Schweigepflicht", sind rechtswidrig. Die Einwilligung kann auch schriftlich erfolgen, z.B. in Form einer Patientenverfügung. Kann der Patient in die Entbindung nicht einwilligen, weil er urteilsunfähig ist, willigt der gesetzliche Vertreter (z.B. Vormund, Beistand, Eltern) ein. Allenfalls muss die Vormundschaftsbehörde eingeschaltet werden, welche entscheidet. Ist kein gesetzlicher Vertreter vorhanden, muss der mutmassliche Wille des betroffenen Patienten unter Einbezug der Meinung enger Familienangehöriger (z.B. Ehegatte, Lebenspartner, Kinder) ermittelt werden;

- Mit schriftlicher Bewilligung des kantonalen Departements des Innern als Aufsichtsbehörde, z.B. wenn ein Arzt oder Spitalpersonal als Zeuge in einem Zivilprozess oder Strafverfahren aussagen soll;

- Bei Vorliegen einer Bewilligung gemäss Art. 321bis StGB: Forschung im Bereich der Medizin oder des Gesundheitswesens;

- Wenn eine gesetzliche Meldepflicht oder ein gesetzliches Melderecht besteht, z.B.: - Pflicht, dem Kantonsarzt aussergewöhnliche Todesfälle zu melden; - Pflicht, dem Kantonsarzt Seuchen und andere ansteckenden Krankheiten zu

  melden;

  Recht der Vormundschaftsbehörde Misstände, die ein Einschreiten zum Zweck des Kindesschutzes und der Jugendfürsorge erfordern, zu melden, z.B. ein Kind hat am Körper ungewöhnlich viele blaue Flecken und die Polizei musste schon zu Hause „Streit" schlichten.

[24] BGS 126.1
[25] SR 311.0

Recht, der Polizei oder Staatsanwaltschaft strafbare Handlungen gegen Leib und Leben, die öffentliche Gesundheit oder die sexuelle Integrität zu melden, z.B. ein Kind hat am Körper viele blaue Flecken, die auf Gewalt zurückzuführen sind; - Pflicht, Geburten / Todesfälle an das Zivilstandsamt zu melden.

- Wenn spezielle gesetzliche Bestimmungen öffentliche Spitäler zur Bekanntgabe von Patientendaten auf Anfrage einer Behörde verpflichten;

Pflicht öffentlicher Spitäler als Leistungserbringer zur Bekanntgabe von notwendigen Patientendaten an Sozialversicherungen, z.B. nach Art. 42 des eidg. Krankenversicherungsgesetzes (KVG).[26]

7. Auskunfts- und Einsichtsrechte des Patienten

7.1 Aufklärung[27]

Der behandelnde Arzt, allenfalls Pflegepersonal, welches dazu legitimiert ist, müssen den Patienten grundsätzlich voll über seinen medizinischen Zustand informieren, also z.B. über diagnostische Untersuchungen, Diagnosen, vorgeschlagene / mögliche Therapien, Risiken und Nebenwirkungen der Behandlung, die voraussichtliche Entwicklung des Gesundheitszustandes mit oder ohne vorgeschlagene Therapie. Das zuständige Spitalpersonal muss den Patienten auch über die Kosten aufklären, z.B. wenn eine Behandlung nicht durch die obligatorische Krankenversicherung abgedeckt ist und der Patient keine Zusatzversicherung hat. Diese grundsätzlich vollumfängliche Aufklärungspflicht umfasst selbstverständlich auch die Beantwortung von Anschlussfragen des Patienten.

Ausnahmsweise muss der Arzt überhaupt nicht, nur teilweise oder erst zu einem späteren Zeitpunkt, allenfalls in Absprache mit den nächsten Angehörigen, aufklären. Hier ist Einfühlungsvermögen und gesunder Menschenverstand gefragt. Als Beispiele können angeführt werden:

- Der Patient möchte (noch) nicht oder nicht ganz informiert werden;
- Der Patient ist urteilsunfähig[28];
  - Sogenannter „Aufklärungsschaden“: Ein Arzt hat die Diagnose „bösartiger Tumor“ im Endstadium. Der Arzt merkt im Rahmen des Gesprächs, dass der Patient akut suizidgefährdet ist oder sonst in psychisch schlechter Verfassung ist. Wenn er nun dem Patienten sofort „reinen Wein“ einschenken würde, würde dieser wahrscheinlich Suizid begehen oder er könnte die volle Wahrheit psychisch nicht mehr verkraften (z.B. Nervenzusammenbruch). Hier beruhigt der Arzt den Patienten besser und wird ihn, wenn überhaupt, erst zu einem späteren Zeitpunkt aufklären.

7.2 Auskunft und Einsicht in Patientendaten

Der urteilsfähige Patient (in der Regel ab dem vollendeten 12. Altersjahr) oder sein Vertreter, z.B. bevollmächtigter Rechtsanwalt, bevollmächtigte Privatperson wie etwa Eltern, Vormund, haben ein Recht auf Auskunft und auf Verlangen ein Recht auf Einsicht in die Patientendaten. Das Einsichtsrecht umfasst auch das Recht eine Kopie oder einen Ausdruck von Patientendaten, z.B. aus dem Spitalinformationssystem hospis, zu verlangen (§ 32 des kantonalen Gesundheitsgesetzes, § 26 InfoDG). Im Dossier muss festgehalten werden, wer was wem wann (Datum) herausgegeben hat.

[26] SR 832.10, siehe Ziffer 8.1, S. 7 ff. dieses Merkblattes
27 § 31 des kantonalen Gesundheitsgesetzes
[28] Siehe Ziffer 6, S. 5 dieses Merkblattes

Der Patient oder sein Vertreter kann das Auskunfts- oder Einsichtsgesuch jederzeit, ohne Begründung, mündlich oder schriftlich bei der für den Datenschutz verantwortlichen Person, z.B. beim behandelnden Pflegepersonal über die Pflege, beim behandelnden Arzt über Details zur Diagnose, stellen. Wenn der Patient nicht persönlich bestens bekannt ist, muss er seine Identität mit einem amtlichen Ausweis (Pass oder Identitätskarte) oder einer Kopie davon nachweisen.29

Grundsätzlich besteht ein Recht auf Auskunft, Einsicht in sämtliche administrativen und medizinischen Daten über den Patienten. Davon gibt es aber Ausnahmen. Beispiele von Ausnahmen:

- Die Einsicht ist zu verweigern für rein persönliche Notizen oder interne Akten, das heisst Gedächtnisstützen, des Arztes, des Pflegepersonals etc., z.B. eine Handnotiz des Arztes zur Vorbereitung eines Gesprächs mit dem Patienten, Agenda-Einträge von Besprechungsterminen wie Teamsitzungen des Arztes, des Pflegepersonals 30 ;
- Die Einsicht ist zu verweigern bei schützenswerten Interessen des Arztes (selten), z.B. wenn viele Schreibfehler in einer Fremdsprache in der Krankengeschichte sind, in diesem Fall muss der Arzt entweder mündlich informieren oder wenn der Patient dies verlangt, den wesentlichen Inhalt der Krankengeschichte in deutscher Sprache schriftlich zusammenfassen und dem Patienten herausgeben;
- Die Einsicht kann im Einzelfall verweigert werden bei persönlichen Angaben von Dritten, aber nur in krassen Fällen, z.B.

Wenn Familienangehörige, Freunde oder Bekannte dem Arzt über Schwächen, die Lebensweise, das Verhalten des Patienten im Bereich der Sexualität Auskünfte gegeben haben, ausser diese haben bewusst falsche Angaben

gemacht oder diese Angaben gegenüber dem Patienten selber auch schon geäussert;

Wenn der Arzt konkret befürchten muss, dass die Drittperson, welche Auskünfte im vorerwähnten Sinne gegeben hat, bei Offenlegung der Auskunft vom Patienten bedroht, tätlich angegriffen oder sonstwie verletzt werden wird; Im Zweifelsfall ist es besser, den Namen der Drittperson oder gar die ganze Passage mit der Auskunft der Drittperson abzudecken, das heisst zu

anonymisieren, wenn der Patient diese trotz Namensabdeckung identifizieren kann (z.B. Ehefra u)31;

- Bei wichtigen öffentlichen Interessen / dem Schutz des betroffenen Patienten vor sich selber, z.B. beim erwähnten „Aufklärungsschaden “32 ist die Einsicht entweder später (das Risiko des „Aufklärungsschadens besteht nicht mehr) oder gar nicht (Risiko des „Aufklärungsschadens“ bleibt) zu gewähren. Es empfiehlt sich, hier allenfalls mit den nächsten Angehörigen Rücksprache zu nehmen. Je nach Einzelfall kann anstelle der Einsicht die Auskunft entweder mündlich oder schriftlich in einem kurzen Bericht (z.B. mit Erläuterung medizinischer Fachausdrücke) erteilt werden.

8. Bekanntgabe von Patientendaten an Dritte

Dritte wünschen Patientendaten häufig für ganz andere Zwecke, als das Spital diese erhoben hat (Zweckbindung). Dritte müssen deshalb gegenüber der für den

[29] § 26 Abs. 1 InfoDG, siehe Muster-Auskunftsgesuch, abrufbar unter www.datenschutz.so.ch - Merkblätter

[30] § 32 Abs. 2 des kantonalen Gesundheitsgesetzes, § 6 Abs. 3 Bst. b InfoDG

[31] Siehe dazu z.B. das Urteil des Schweizerischen Bundesgerichts vom 19.06.1996 bezüglich Einsicht in eine Psychiatrie-Krankengeschichte in Sachen M. gegen Psychiatrische Klinik Schlössli Oetwil a.S. und Regierungsrat des Kantons Zürich, BGE 122 I 153 ff., abrufbar unter www.bger.ch.

[32] Siehe Ziffer 7. 1, S. 6 dieses Merkblattes

Datenschutz verantwortlichen Person – auf Verlangen schriftlich - begründen, dass sie die gewünschten Patientendaten bearbeiten dürfen, z.B. durch ihren gesetzlichen Auftrag (Behörden) oder eine ausdrückliche Einwilligung des betroffenen Patienten. Sie müssen zudem begründen, dass sie diese Patientendaten auch tatsächlich benötigen (Verhältnismässigkeit).

Die für den Datenschutz verantwortliche Person darf Patientendaten an Dritte nur bekanntgeben, z.B. mündliche Auskünfte erteilen, einen ärztlichen Bericht verfassen und herausgeben, Einsicht geben, Ausdrucke aus dem Spitalinformationssystem hospis oder Kopien von papierenen Patientendaten herausgeben, wenn die allgemeinen datenschutzrechtlichen Grundsätze sowie das Patientengeheimnis bzw. Berufsgeheimnis und/oder das Amtsgeheimnis nicht verletzt werden.

8.1 Beispiele für die Bekanntgabe von Patientendaten an Behörden

- Gesetzliche Meldepflichten und Melderechte;[33]

- An den Spitalrat, die Spitalleitung, anderen Leitungsgremien innerhalb des öffentlichen Spitals, Vorgesetzte
  Im Rahmen ihrer Zuständigkeit müssen kraft Aufsichtsfunktion im Einzelfall auch die notwendigen Patientendaten an diese Stellen weitergeleitet werden. Dabei ist jeweils das Verhältnismässigkeitsprinzip einzuhalten. Die Stellen sind ebenfalls an die Schweigepflicht gebunden.

Beispiele:

- Für die Stellungnahme zu einer Aufsichtsbeschwerde eines Patienten gegen das behandelnde Pflegepersonal oder den behandelnden Arzt, in welcher diesen ärztliche Kunstfehler angelastet werden, haben diese Stellen das Recht, die gesamte Krankengeschichte im Original zu konsultieren, Kopien einzusehen und Auskünfte einzuholen. Nur so können sie richtig entscheiden, wie die Stellungnahme abzufassen ist. Dies gilt auch für spitalinterne Aufsichtsstellen (z.B. mit Ombudsfunktion), damit diese den Sachverhalt erheben und einen sachgerechten Entscheid fällen können.
- Im operationellen Bereich ist es zulässig, dass z.B. ein Einzelfall in der Chefärztekonferenz, in der Klinik- oder Abteilungskonferenz, im Team oder dem Vorgesetzten vollumfänglich geschildert wird, um die für den Patienten richtige Behandlung zu evaluieren (Vier- oder Mehraugenprinzip).
- Reine Statistiken über die Anzahl behandelter Patienten etc. dürfen grundsätzlich nur in anonymisierter Form an den Spitalrat, die Spitalleitung weitergegeben werden.

- An andere Abteilungen, Kliniken innerhalb desselben öffentlichen Spitals: Dies ist zulässig, sofern die Auskünfte, schriftlichen medizinischen Daten wirklich benötigt werden. Dies ist etwa der Fall, wenn Ärzte, Pflegepersonal, andere Abteilungen, Kliniken, den Patienten mitbehandeln, weiterbehandeln, nachbehandeln (§ 33 Abs. 2 Bst. b des kantonalen Gesundheitsgesetzes). Z.B. muss der im öffentlichen Spital angestellte Physiotherapeut die Diagnose und Begleitinformationen dazu vom behandelnden Arzt wissen, um mit einem wegen eines Hirnschlags einseitig gelähmten Patienten eine auf dessen gesundheitliche Situation angepasste Physiotherapie planen und beginnen zu können.

[33] Siehe Ziffer 6, S. 4ff. dieses Merkblattes

An ein anderes Spital, in welches der Patient verlegt wurde:
Die Bekanntgabe an jedes andere Spital (privat34 oder öffentlich spielt keine Rolle) unter den gleichen Voraussetzungen und im gleichen Umfang wie innerhalb des öffentlichen Spitals, ist ebenfalls zulässig (§ 33 Abs. 2 Bst. b des kantonalen Gesundheitsgesetzes).

An die Spitex:
Auch hier ist eine Bekanntgabe der notwendigen medizinischen Daten gemäss § 33 Abs. 2 Bst. b des kantonalen Gesundheitsgesetzes erlaubt. Es genügen in der Regel mündliche Auskünfte über den Gesundheitszustand des Patienten (Diagnose),
welche Medikamente er einnehmen muss oder allenfalls ein ärztlicher Bericht, in welchem das wichtigste für die Pflege zusammengefasst ist.

An die obligatorische Krankenkasse (Grundversicherung):
Krankenkassen gelten im obligatorischen Bereich (Grundversicherung) als „Bundesorgan".35 Öffentliche Spitäler müssen der obligatorischen
Krankenversicherung gemäss speziellen Gesetzesbestimmungen, Art. 42 des eidg. Krankenversicherungsgesetzes, KVG, § 16 Abs. 1 Bst. a InfoDG medizinische Patientendaten weitergeben.

Personenbezogene medizinische Patientendaten (Rückschluss, wer der Patient ist, ist möglich):
Krankenkassen haben keinen Online-Zugriff auf das Spitalinformationssystem hospis, können also Patientendaten nicht elektronisch abrufen;

Im ambulanten Bereich (Tarifsystem Tarmed) werden systematisch in den Spitalrechnungen keine Diagnosedaten - auch nicht in Form der Codes der Internationalen statistischen Klassifikation der Krankheiten und verwandter Gesundheitsprobleme in der Fassung der 10. Revision, dem sogenannten ICD-10- Code – aufgeführt. Stattdessen werden Diagnose-Daten jeweils an den Vertrauensarzt der obligatorischen Krankenkasse übermittelt.

An obligatorische Krankenkassen werden zudem folgende Daten
weitergegeben, damit jene ihre Leistungspflicht (Übernahme der Kosten des Spitals) prüfen können: Leistung KVG ja/nein, Leistung Haftpflichtversicherung ja/nein, Leistung Unfallversicherung ja/nein.

In Einzelfällen dürfen zwecks Prüfung der Leistung weitere detailliertere medizinische Daten, insbesondere die genaue Diagnose und/oder zusätzliche medizinische Auskünfte an die obligatorische Krankenkasse weitergegeben werden (Art. 42 Abs. 3 KVG).

Der Patient kann auch verlangen, dass das öffentliche Spital alle medizinischen Angaben nur an den Vertrauensarzt weitergibt (Art. 42 Abs. 5 KVG). Der Vertrauensarzt prüft vor allem, ob die obligatorische Krankenkasse aus medizinischer Sicht die Kosten ganz oder nur teilweise für den Spitalaufenthalt übernehmen muss. Die obligatorische Krankenkasse kann ihm keine Weisungen erteilen. Der Vertrauensarzt ist also völlig unabhängig und er darf der obligatorischen Krankenkasse nur medizinische Patientendaten weitergeben,

[34] Privatspitäler, also solche ohne Leistungsauftrag des Kantons Solothurn sind keine „Behörden" im datenschutzrechtlichen Sinne gemäss § 3 Bst. c InfoDG. Für sie als „Private" gelten die Art. 12 ff. des eidg. Datenschutzgesetzes (DSG, SR 235.1).
[35] Art. 3 Bst. h des eidg. Datenschutzgesetzes (DSG)

wenn er dies für notwendig erachtet und falls ja, nur im benötigten Umfang (Art. 57 KVG);

- Im stationären Bereich leitet das Spital vor oder nach Spitaleintritt jeweils ein Gesuch um Kostengutsprache mit der Klartextdiagnose (allgemeine Diagnose, z.B. Lungenentzündung, aus den ICD-10-Codes sind viel mehr medizinische Daten über die Krankheit ableitbar als aus der Klartextdiagnose) direkt der Versicherung weiter.

  Im weiteren erhalten die obligatorischen Krankenkassen wie im ambulanten Bereich nur die notwendigen medizinischen Daten. Also auch im stationären Bereich werden die Diagnose-Daten nicht systematisch in der Spitalrechnung aufgeführt und der Krankenkasse übermittelt, weil dies gar nicht notwendig ist.

  Im übrigen darf das Spital selbstverständlich im Einzelfall detailliertere medizinische Daten, z.B. Operationsberichte, Austrittsberichte, an die obligatorische Krankenversicherung weitergeben, wenn dies wirklich nötig ist.

  Der Patient kann auch im stationären Bereich verlangen, dass medizinische Daten nur an den Vertrauensarzt weiterzuleiten sind (Art. 42 Abs. 5 KVG).

- An die obligatorische Unfallversicherung:
  Personenbezogene medizinische Daten (Rückschluss, wer der Patient ist, ist möglich): Das öffentliche Spital übermittelt der obligatorischen Unfallversicherung (z.B. SUVA) im Gegensatz zur obligatorischen Krankenkasse regelmässig eine detaillierte und verständliche Spitalrechnung mit der genauen Diagnose (Art. 54a des Bundesgesetzes über die Unfallversicherung, UVG[36], und Art. 69a der eidg. Verordnung über die Unfallversicherung, UVV[37]).

  Darüberhinaus muss das öffentliche Spital im Einzelfall nur weitere medizinische Angaben machen, wenn die Unfallversicherung begründen kann, dass sie diese benötigt, um zu prüfen, ob sie überhaupt zahlen muss (liegt ein Unfall vor?) und falls ja, ob die Rechnung in dieser Höhe gerechtfertigt ist.

  Daraus folgt, dass etwa ärztliche Verlaufsberichte, Operationsberichte oder Austrittsberichte nicht regelmässig, sondern nur im begründeten Einzelfall direkt an die obligatorische Unfallversicherung weitergeleitet werden dürfen.[38] Im Kanton Solothurn werden aber im Sinne einer pragmatischen Lösung, welche sowohl die Persönlichkeitsrechte der Patienten als auch die Interessen der Unfallversicherer berücksichtigt, systematisch Verlaufs- und Austrittsberichte jeweils an den Vertrauensarzt der obligatorischen Unfallversicherung zugestellt. Dieser gibt diese der Unfallversicherung aber nur weiter, wenn dies im Einzelfall wirklich notwendig ist. Den Nachweis, dass diese effektiv benötigt werden, muss die obligatorische Unfallversicherung erbringen.

- An die Invalidenversicherung (IV)
  Der Patient, der IV-Leistungen beansprucht, hat die kantonale IV-Stelle zu ermächtigen, beim öffentlichen Spital die für die Abklärung von Leistungsansprüchen

[36] SR 832.20
[37] SR 832.202
[38] So auch die Vereinigung der Schweizerischen Datenschutzbeauftragten DSB+CPD.CH in ihrem Merkblatt „Austritts- und Operationsberichte“ vom Juni 2002, abrufbar unter www.dsb-cpd.ch, und der eidg. Datenschutzbeauftragte in seinem 10. Tätigkeitsbericht 2002/2003, Herausgabeflicht der Leistungserbringer nach UVG, S. 54, abrufbar unter www.edsb.ch.

erforderlichen Auskünfte zu erteilen. Soweit die medizinischen Daten nötig sind, ist das öffentliche Spital verpflichtet, Auskunft zu geben. Die Auskunft kann mündlich oder schriftlich, z.B. in einem ärztlichem Bericht, gegeben werden (Art. 28 Abs. 2 und 3 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts, ATSG39). Daten, welche die Privatsphäre oder Intimität des Patienten betreffen und überhaupt nicht in einem Zusammenhang mit einer IV-Leistung stehen, wie z.B. zum Verhalten des Patienten, benötigt die kantonale IV-Stelle hingegen nicht.

Zudem kann die kantonale IV-Stelle beim öffentlichen Spital die erwähnten medizinischen Daten auch schriftlich im Einzelfall auf dem Amtshilfeweg verlangen. Sie muss dabei begründen, dass sie die medizinischen Daten zur Festsetzung, Änderung oder Rückforderung von Leistungen, zur Verhinderung ungerechtfertigter Bezüge oder zum Rückgriff auf haftpflichtige Dritte benötigt. Dies setzt aber voraus, dass der Patient keine Vollmacht erteilt hat (Art. 32 Abs. 1 Bst. a, b und d ATSG, Art. 66 des Bundesgesetzes über die Invalidenversicherung, IVG40 und Art. 49a Abs. 1 Bst. b, d des Bundesgesetzes über die Alters- und Hinterlassenenversicherung, AHVG41).

O An die Ausgleichskasse des Kantons Solothurn (Ergänzungsleistungen)

Für die Bekanntgabe von medizinischen Patientendaten an die Ausgleichskasse des Kantons Solothurn gilt auch das bei Invalidenversicherung Gesagte. 42

O An die Sozialhilfebehörde

Die Sozialhilfebehörde muss im Einzelfall ein schriftlich begründetes Gesuch beim öffentlichen Spital stellen. Darin muss sie präzisieren, welche medizinische Daten des Patienten sie für die Festsetzung, Änderung oder Rückforderung von Leistungen beziehungsweise für die Verhinderung ungerechtfertigter Bezüge benötigt (Art. 84a Abs. 1 Bst. h Ziff. 1 des eidg. Krankenversicherungsgesetzes, KVG).

Im Normalfall genügen folgende medizinischen Daten vollkommen: - Spitalrechnungen;
- Entscheide betreffend Spitalrechnungen;
- Ausnahmsweise ein ärztlicher Bericht.

O An das kantonale Departement des Innern als Aufsichtsbehörde

Für die Spitalplanung, den Abschluss und die Überprüfung der Leistungsverein-barung müssen die öffentlichen Spitäler dem kantonalen Departement des Innern die nötigen Daten und Auskünfte zur Verfügung stellen. Dieses prüft dann etwa deren Kostendeckungsgrad, Wirtschaftlichkeit etc. in regelmässigen Zeitabständen (§§ 11 und 14 des kantonalen Spitalgesetzes, §§ 46 und 47 des kantonalen Gesundheitsgesetzes). Dafür genügen anonymisierte Patientendaten vollständig.

Bei der übrigen Aufsicht, z.B. der schriftlichen Entbindung des Arztes vom Patienten- bzw. Berufsgeheimnis und Amtsgeheimnis oder bei der Behandlung von Aufsichtsbeschwerden gegen einen Spitalmitarbeiter, welche die medizinische Behandlung betreffen, muss das kantonale Departement des Innern volle Einsicht in alle administrativen und medizinischen Patientendaten, das heisst also auch in die Krankengeschichte, erhalten.

[39] SR 830.1
[40] SR 831.201
[41] SR 831.10
[42] Siehe weitere Informationen zu Ergänzungsleistung auf der Homepage der Ausgleichskasse des Kantons Solothurn unter www.akso.ch.

An die Kantonspolizei, Staatsanwaltschaft (Strafverfolgungsbehörden)
Sofern bei den Strafverfolgungsbehörden eine Strafanzeige wegen fahrlässiger Tötung, Körperverletzung, sexuellem Missbrauch, etc. erstattet wurde, müssen diese den Sachverhalt von Amtes wegen abklären.

Das öffentliche Spital ist im Einzelfall und auf schriftlich begründetes Gesuch hin verpflichtet, der Kantonspolizei oder der Staatsanwaltschaft die Daten, die für die Abklärung solcher Vergehen und Verbrechen erforderlich sind, bekannt zu geben (Art. 84a Abs. 1 Bst. h Ziff. 3 des eidg. Krankenversicherungsgesetzes, KVG). Je nach
Einzelfall kann dies ein ärztlicher Bericht oder die ganze Krankengeschichte sein.

Zudem können Ärzte, Pflegepersonal, welche sachdienliche Hinweise geben können, auch als Zeugen einvernommen werden. Sie müssen allerdings vom kantonalen Departement des Innern vom Patientengeheimnis und Amtsgeheimnis entbunden sein. Im Strafprozess haben sie trotz Entbindung vom Amts- und Patienten- resp. Berufsgeheimnis ein Zeugnisverweigerungsrecht (§ 64 der kantonalen
Straf prozessordnung[43]). Ein behandelnder Arzt oder Spitalpersonal, gegen welche selber ein Strafverfahren läuft, können sich nicht auf dieses Zeugnisverweigerungsrecht berufen.

- An Gerichte
  Im Einzelfall muss das öffentliche Spital auf schriftlich begründetes Gesuch auch medizinische Daten an das zuständige Gericht herausgeben (Art. 84a Abs. 1 Bst. h Ziff. 3 und 4 des eidg. Krankenversicherungsgesetzes, KVG) bekanntgeben:
  - Zivilgerichte, wenn die Daten für die Beurteilung eines familien- oder erbrechtlichen Streitfalles erforderlich sind;
  - Strafgerichte, Strafuntersuchungsbehörden soweit die Daten für die Abklärung eines Verbrechens oder Vergehens nötig sind.

  Im Übrigen sind auch hier die Bestimmungen des Zeugnisverweigerungsrechtes im Strafprozess und im Zivilprozess (§ 172 Abs. 1 Bst. b der kantonalen Zivilprozessordnung[44]) zu beachten.

- An die Pfarrer der im Kanton Solothurn öffentlich-rechtlichen anerkannten Kirchen Eine Bekanntgabe des Namens, Vornamens, Geburtsdatums und der Adresse an den zuständigen Pfarrer (katholische, reformierte, christkatholische Kirche), aber nur bezüglich Patienten ihrer Kirchgemeinde, ist zulässig. Voraussetzung ist, dass ein Patient z.B. im Informationsblatt die Frage der Weitergabe seines Namens, Vornamens, Geburtsdatums, seiner Adresse an einen Seelsorger ausdrücklich bejaht hat.[45]

- An andere Behörden
  Im Übrigen ist eine Bekanntgabe von Patientendaten nur mit vorgängiger schriftlicher Einwilligung des betroffenen Patienten oder wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Patienten vorausgesetzt werden darf, erlaubt (Art. 84a Abs. 5 Bst. b des eidg. Krankenversicherungsgesetzes).

[43] BGS 321.1
[44] BGS 221.1
[45] Weitere Informationen dazu im Merkblatt „Datenschutz in den Kirchgemeinden und den öffentlichrechtlich anerkannten Kirchen des Kantons Solothurn“, S. 2, abrufbar unter www.datenschutz.so.ch - Merkblätter

8.2 Beispiele für die Bekanntgabe von Patientendaten an Private

An nächste Angehörige, Ehepartner, Lebenspartner
Grundsätzlich darf Auskunft über den Patienten selber nur mit dessen Einverständnis erteilt werden. Behandelnde Ärzte, Pflegepersonal etc. dürfen aber vermutungsweise den nächsten Angehörigen wie urteilsfähigen Kindern, Eltern, dem Ehepartner oder Lebenspartner des Patienten Auskünfte über den Gesundheitszustand, die Behandlung, die Heilungsaussichten geben, sofern aus den Umständen nicht auf einen Geheimhaltungswillen des Patienten geschlossen werden muss (§ 33 Abs. 2 Bst. a des kantonalen Gesundheitsgesetzes). Dies umfasst auch das Recht, die Krankengeschichte einsehen zu dürfen.

Es muss grundsätzlich offen, also vollständig informiert werden. Ausnahmen davon sind dieselben wie beim Patienten selber, im Vordergrund steht der bereits erwähnte „Aufklärungsschaden".46 Ist der Patient verstorben, haben erbberechtigte Angehörige grundsätzlich auch ein volles Auskunfts- und Einsichtsrecht, um z.B. die Testierfähigkeit abklären zu können. Hier genügt in der Regel ein ärztlicher Bericht.

Zu beachten ist auch, dass mit dem Tod eines Patienten die nächsten Angehörigen in den Entscheidprozess, ob Privaten Auskunft oder Einsicht in medizinische Daten des Verstorbenen gewährt werden soll, einzubeziehen sind (sogenanntes Recht auf „Andenkensschutz"). Soweit also die Adresse naher Angehöriger bekannt ist, ist es empfehlenswert, diese um ihre Stellungnahme zum Auskunfts- oder Einsichtsgesuch zu bitten.

An Hausarzt, spezialisierten Arzt, Physiotherapeuten, etc.
Die medizinisch notwendigen Auskünfte müssen an die sogenannten Heilpersonen, also Hausärzte, Spezialärzte, Physiotherapeuten, Spitex etc., welche zuweisen, mitbehandeln, nachbehandeln oder an der Therapie beteiligt sind, bekanntgegeben werden (§ 33 Abs. 2 Bst. b des kantonalen Gesundheitsgesetzes). In den meisten Fällen wird ein ärztlicher Bericht genügen.

An Haftpflichtversicherungen, andere Privatversicherungen
Haftpflichtversicherungen, andere Privatversicherungen wie z.B. Zusatzversicherungen zur obligatorischen Krankenversicherung, müssen ebenfalls beurteilen, ob sie Spitalkosten bezahlen müssen und falls ja, in welcher Höhe. Daneben sind für sie aber medizinische Daten interessant, da sie mögliche Kunden mit einem hohen Risiko ablehnen können (z.B. Daniel Schmid, 80-jährig, starker Raucher, hospitalisiert wegen eines Lungenleidens, das auf das starke Rauchen zurückzuführen ist) oder nur mit Auflagen aufnehmen können, z.B. mit der Pflicht, höhere Prämien zu bezahlen. Oder sie können das erstellte Gesundheitsprofil dazu verwenden, dass z.B. „kerngesunde" Kunden gezielt beworben werden (Marketing).

Das öffentliche Spital darf Privatversicherungen deshalb ausschliesslich für die Schadenabwicklung und nur mit schriftlicher Ermächtigung des Patienten medizinische Daten, die notwendig sind, an die Haftpflichtversicherung, Privatversicherung weitergeben. Wenn die schriftliche Einwilligung nicht möglich ist (z.B. der Patient ist im Koma oder ist urteilsunfähig), können die notwendigen medizinischen Daten dennoch herausgegeben werden, wenn dies der mutmassliche Wille des Patienten ist (Art. 84a Abs. 5 Bst. b des eidg. Krankenversicherungs-gesetzes, KVG). Regelmässig wird in solchen Fällen vorgängig die Meinung des Ehepartners oder Lebenspartners und anderer nächster Angehöriger eingeholt.

46 Siehe Ziffer 7.1 S. 6 und Ziffer 7.2 S. 7 dieses Merkblattes

Welche medizinischen Daten dürfen herausgegeben werden? Im Normalfall genügt ein ärztlicher Bericht.

An übrige Private

An übrige natürliche Personen oder Firmen, wie z.B. Pharmafirmen etc., dürfen Patientendaten, insbesondere auch Daten aus der Krankengeschichte, ebenfalls nur mit schriftlicher Ermächtigung des Patienten weitergegeben werden. Wenn dies nicht möglich ist, ist auch hier der mutmassliche Wille des Patienten unter Beizug des Ehepartners respektive des Lebenspartners sowie der nächsten Verwandten zu ergründen. Nur wenn dieser bejaht wird, dürfen die benötigten Patientendaten bekanntgegeben werden (Art. 84a Abs. 5 Bst. b des eidg. Krankenversicherungsgesetzes, KVG).

Der Beauftragte für Information
und Datenschutz des Kantons Solothurn

sig. Daniel Schmid / 13.12.2007

4.15 Anhang 15: Präsentationsbewertung

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Wirtschaft

Bewertung Präsentation Fallstudie Risikomanagement

Die Präsentation soll bewertet werden, damit das Engagement belohnt wird. Mit der nachfolgenden Liste wird versucht, einheitliche Kriterien für die Beurteilung zu schaffen. Die aus der Summe der Punkte ermittelte „Note" muss dem Gesamteindruck entsprechen, ansonsten ist die Note zu Gunsten der Studierenden zu korrigieren.

Student/in: Name: _____ Vorname: _____

Präsentation (Total 12 Punkte)	erfüllt	teilweise erfüllt	nicht erfüllt	Bemerkungen
- bewusster Augenkontakt	1	½	0	
- dynamische Sprache	2	1	0	
- Fragen unterwegs	1	½	0	
- überzeugend	1	½	0	
- Hilfsmittel angepasst eingesetzt	1	½	0	
- Diskussion geleitet	2	1	0	
- Aufforderung zur Tat	2	1	0	
- Einbezug des Publikums (wir)	1	½	0	
- Körperhaltung (ruhig)	1	½	0	
Total				
Vermittlung Inhalt (Total 8 Punkte)				
- entspricht schriftlichen Version / wesentliche Aussagen erwähnt	2	1	0	
- publikumsgerechte Ausführungen	2	1	0	
- Zeitvorgaben eingehalten (20 Min +/-1 Min)	2	1	0	
- Slides aufs Wesentliche konzentriert	2	1	0	

Total Punkte = Anzahl Punkte / 4
(Aufrunden auf ganze Zahl):

Persönliche Bemerkungen (bei Bedarf die Rückseite benutzen):

Datum / Unterschrift

FH Zentralschweiz

EFQM