Anforderungen hinsichtlich der anlassbezogenen und anlasslosen Datenschutzkontrolle an Protokollierungen

Erarbeitet von

Bundesverband Gesundheits-IT e.V.
Arbeitsgruppe „Datenschutz & IT-Sicherheit“

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Gesellschaft für Datenschutz und Datensicherheit e.V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Version 1.0

Stand der Bearbeitung: 02. Juli 2022

Autoren (alphabetisch)

Jamie Crookes	Compliant Digital GmbH & Co. KG
Siegfried Hellmich	Deutsche Telekom Clinical Solutions GmbH
Christoph Isele	Cerner Deutschland GmbH
David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Tatjana Neitz-Kluge	Medizinische Hochschule Hannover (MHH)
Mark Rüdlin	Datenschutzbeauftragter und Rechtsanwalt
Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security Solutions GmbH
Gerald Spyra	Sozietät Ratajczak & Partner mbB

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Inhaltsverzeichnis

Vorwort

Entsprechend Art. 39 DS-GVO gehört zu den Aufgaben eines Datenschutzbeauftragten die Überwachung der Einhaltung der Datenschutzregelungen.

In Art. 39 Abs. 2 DS-GVO ist zudem der risikobasierte Ansatz der DS-GVO abgebildet worden, sodass der Datenschutzbeauftragte die Erfüllung seiner Aufgaben und insbesondere die Bewertungen der technischen und organisatorischen Maßnahmen am Risiko ausrichten muss, welches die jeweilige Verarbeitung für die Rechte und Freiheiten betroffener Personen beinhaltet. Dieser risikoorientierte Ansatz verlangt vom Datenschutzbeauftragten unter anderem, dass die Aufgaben mit „Augenmaß" bearbeitet werden. Zum risikoorientierten Ansatz gehört jedoch gleichermaßen, dass er kritische Datenverarbeitungen in den Mittelpunkt seiner Tätigkeit stellt[1].

ErwGr. 51 DS-GVO sieht bei besonderen Kategorien von personenbezogenen Daten einen besonders hohen Schutzbedarf: „Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können." Art. 9 Abs. 1 DS-GVO benennt diese besonderen Datenkategorien:

- Daten, aus denen die rassische und ethnische Herkunft hervorgeht,
- Daten bzgl. politischer Meinungen,
- Daten hinsichtlich religiöser oder weltanschaulicher Überzeugungen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung.

Eine Verarbeitung von Gesundheitsdaten und/oder genetischen Daten(-kategorien) beinhaltet entsprechend ErwGr. 51 DS-GVO also immer „erhebliche Risiken für die Grundrechte und Grundfreiheiten" betroffener Personen, d. h. bei einer Verarbeitung dieser Daten muss grundsätzlich von einem hohen Schutzbedarf ausgegangen werden, welcher besondere Maßnahmen zur Gewährleistung eines entsprechend hohen Sicherheitsniveaus verlangt.

Dementsprechend gehören derartige Verarbeitungen zu den kritischen Verarbeitungen, die ein Datenschutzbeauftragter in den Mittelpunkt seiner Tätigkeit stellen muss. Und natürlich muss bei entsprechenden Verarbeitungen eine Überwachung der Einhaltung der Datenschutzregelungen erfolgen. Regelhaft werden zur Verarbeitung dieser Daten Informationssysteme wie ein Krankenhaus-Informationssystem (KIS), Praxis-Verwaltungssystem (PVS), klinisches Arbeitsplatzsystem (KAS) usw. eingesetzt. In diesen Fällen bedingt eine Überwachung der Einhaltung der Datenschutzregelungen immer auch die Kontrolle protokollierter Ereignisse. Dies kann zum einen anlassbezogen erfolgen, wenn beispielsweise eine Beschwerde bzgl. einer möglicherweise rechtswidrigen Verarbeitung von personenbezogenen Daten durch eine betroffene Person eingegangen ist. Zum anderen muss aber stets auch anlassunabhängig eine Kontrolle erfolgen – die in der DS-GVO verankerte Überwachungspflicht des Datenschutzbeauftragten verlangt dies.

In dieser Praxishilfe wird beschrieben, welchen inhaltlichen Anforderungen Protokollierungen in IT-Systemen, mit denen Gesundheitsdaten und/oder genetische Daten verarbeitet werden, genügen müssen, damit Verantwortliche ihren aus dem Datenschutzrecht resultierenden gesetzlichen Pflichten nachkommen können.

[1] Drews S.: Art. 39 Rn. 39. In Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag. 1. Auflage 2019. ISBN 978-3-8487-3590-7

Abgrenzung

Neben dem Datenschutzrecht gibt es auch rechtliche Anforderungen aus dem Bereich der IT-Sicherheit:

- § 8a BSIG verpflichtet Betreiber Kritischer Infrastrukturen, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“, was zwingend eine Protokollierung sicherheitskritischer Ereignisse bedingt.
- Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) bzw. deren Umsetzung in § 8c BSIG beinhaltet für Anbieter von digitalen Diensten die Anforderung, „geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme“ zu bewältigen; auch dies verlangt zwingend eine Protokollierung sicherheitskritischer Ereignisse.
- § 75b SGB V verlangt von an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringern, also insbesondere von allen niedergelassenen Ärzten und Zahnärzten, aber auch von im Krankenhaus erbrachten Leistungen, wie sie in Ambulanzen oder einem MVZ erbracht werden, die Einhaltung einer von der Kassenärztlichen bzw. Kassenzahnärztlichen Bundesvereinigung herausgegebenen und jährlich anzupassenden Richtlinie zur IT-Sicherheit, welche dem Stand der Technik entsprechen muss – was ebenfalls eine Protokollierung sicherheitskritischer Ereignisse verlangt.
- Seit dem 1. Januar 2022 sind Krankenhäuser entsprechend § 75c SGB V verpflichtet, dem Stand der Technik genügende „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“; auch dies erfordert zwingend eine Protokollierung sicherheitskritischer Ereignisse.
- § 19 TTDSG verlangt von Anbietern von Telemedien, u. a. durch technische und organisatorische Vorkehrungen, sicherzustellen, dass Nutzer dieser Telemedien diese gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können – was eine Detektion sicherheitskritischer Ereignisse verlangt, also deren Protokollierung.
  Da dieses Gesetz für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 61 TKG, telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder Rundfunk nach § 2 des RStV sind, gilt und somit bspw. auch für Webseiten gelten können, ist hiervon nahezu jedes Unternehmen betroffen.

Für Banken existieren ebenfalls entsprechende regulatorische Anforderungen, desgleichen für die Energiewirtschaft und auch weitere Sektoren. Unabhängig von diesen spezialgesetzlichen Regelungen erwachsen auch schon aus zivilrechtlichen Generalklauseln, welche Haftungsfragen adressieren, Verpflichtungen zur Gewährleistung von IT-Sicherheit, die regelhaft eine Protokollierung sicherheitskritischer Ereignisse beinhaltet.

Die Protokollierung sicherheitskritischer Ereignisse kann die Verarbeitung von Daten erfordern, welche für die Gewährleistung datenschutzrechtlicher Pflichten nicht erforderlich sind. Diese Arbeit beschäftigt sich ausschließlich mit den zur Erfüllung datenschutzrechtlicher Pflichten erforderlichen Daten.

Hinweise:

1) Auch eine Protokollierung zur Gewährleistung rechtlicher Vorgaben zur IT-Sicherheit unterliegt den in Art. 5 DS-GVO enthaltenen Vorgaben, insbesondere

- muss die Verarbeitung in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden, d. h. es muss vor allem beschrieben werden,
    a) welche rechtlichen Grundlagen die Protokollierung erlauben oder sogar erfordern,
    b) was, zu welchen Zeitpunkten, aus welchen Gründen protokolliert wird,
    c) wer auf diese Protokolldaten, wann aus welchen Gründen, unter welchen Bedingungen zugreifen darf
    d) und für wie lange die Daten gespeichert werden

  (Art. 5 Abs. 1 lit. a DS-GVO, „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- dürfen diese Daten ausschließlich zu Zwecken der IT-Sicherheit genutzt werden
  (Art. 5 Abs. 1 lit. b DS-GVO, „Zweckbindung“);
- muss die Protokollierung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein, was insbesondere eine Dokumentation der zu protokollierenden Daten inkl. der Darstellung der Notwendigkeit erfordert; eine anlasslose Speicherung aller denkbaren Daten für den Fall, dass man diese einmal evtl. gebrauchen kann, ist somit auch aus Gründen der IT-Sicherheit regelmäßig rechtswidrig
  (Art. 5 Abs. 1 lit. c DS-GVO, „Datenminimierung“);
- müssen Daten in einer Form gespeichert werden, welche die Identifizierung der von der Verarbeitung betroffenen Personen nur so lange ermöglicht, wie es für die mit der Verarbeitung zu erreichenden Zwecke erforderlich ist, d. h. Daten müssen so früh wie möglich entweder gelöscht oder anonymisiert werden
  (Art. 5 Abs. 1 lit. e DS-GVO, „Speicherbegrenzung“);
- muss eine angemessene Sicherheit der personenbezogenen Daten gewährleistet werden, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung
  (Art. 5 Abs. 1 lit. f DS-GVO, „Integrität und Vertraulichkeit“).

D. h. es muss ein Protokollierungskonzept[2] existieren, was all diese Punkte und ggf. weitere vorhandene normative Rahmenbedingungen abbildet, und welches einer regelmäßigen Überprüfung unterliegt. Auch muss im Bedarfsfall sichergestellt sein, dass eine Anpassung des Protokollierungskonzeptes und natürlich auch der Protokollierung selbst an geänderte Rahmenbedingungen erfolgt.

2) Eine Protokollierung aus datenschutzrechtlichen Gründen und eine Protokollierung zur Gewährleistung der Einhaltung der Vorgaben zur Erfüllung normativer Vorgaben aus dem Bereich der IT-Sicherheit stellen unterschiedliche Zwecke dar, was ggf. auch eine unterschiedliche Aufbewahrungsdauer zur Folge haben kann. Auch in diesen Fällen gilt Art. 5 Abs. 1 lit. e DS-GVO, sodass nur erforderliche Daten aufbewahrt werden dürfen, d. h. ggf. müssen aus den Protokolldaten für die Zweckerreichung nicht erforderliche Daten gelöscht werden (können), entsprechende technische Möglichkeiten müssen vorhanden sein, wenn eine einzige Protokollierung mehreren Zwecken, die unterschiedliche Aufbewahrungszeiten beinhalten, dient. Ggf. ist es daher sinnvoller, verschiedene Protokolldateien für verschiedene Zwecke zu erstellen.

[2] Zur Erstellung eines Protokollierungskonzeptes bzw. hinsichtlich des Aufbaus und der Struktur eines entsprechenden Konzeptes siehe z. B. die „Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen“ von GMDS, bvitg und IHE. [Online] 2020 [Zitiert 2021-12-28] Verfügbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php

1 Einleitung

Schon die „Orientierungshilfe Krankenhausinformationssysteme“ [3] (OH KIS) forderte im Abschnitt „Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen „eine Protokollierung sowie eine Datenschutzkontrolle, im Abschnitt „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ wurden die Anforderungen an die Protokollierung im Kapitel 7 detaillierter dargestellt.

Eine Protokollierung ist insbesondere aus zwei rechtlichen Vorgaben erforderlich:

1) Verantwortliche müssen gemäß Art. 15 DS-GVO betroffenen Personen auf deren Antrag hin Auskunft erteilen, welche Daten zu ihrer jeweiligen Person gespeichert wurden, wer die Daten zu welchen Zwecken wann verarbeitete, wem die Daten ggfs. weitergegeben wurden usw.
2) Datenschutzbeauftragte müssen entsprechend Art. 39 DS-GVO eine Überwachung der Einhaltung der Datenschutzregelungen bei Verarbeitungen durchführen. Hierzu ist beim Einsatz von Informationssystemen eine Protokollierung erforderlich.

Genaugenommen schreibt die DS-GVO, aufgrund der Tatsache, dass sie technologie-neutral konzipiert wurde, natürlich keine Protokollierung und somit auch nicht die Art und Weise einer Protokollierung vor, sondern benennt nur die Anforderungen – wie Verantwortliche diese Anforderungen umsetzen, ist nicht geregelt. Mitunter wird als Argument für das Erfordernis einer Protokollierung das Urteil des Europäischen Gerichtshof für Menschenrechte aus dem Jahr 2008[4] im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems herangezogen. In der Urteilsbegründung[4] wird dargestellt, dass medizinische Daten zu schützen sind, sei es durch ein entsprechendes Berechtigungskonzept ***oder*** durch entsprechende Protokollierung:

Rn.	Originaltext	Eigene Übersetzung
32	[...] Furthermore, although the legislation did not contain any detailed provisions on the keeping and retention of log-in files, the data controller had a general legal obligation to control the use of personal data files. […]	[...] Auch wenn die Rechtsvorschriften keine detaillierten Bestimmungen über die Aufbewahrung und Speicherung von Log-in-Dateien enthielten, war der für die Verarbeitung Verantwortliche allgemein gesetzlich verpflichtet, die Verwendung von Dateien mit personenbezogenen Daten zu kontrollieren. [...]
44	[...] It is plain that had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, [...]	[...] Es liegt auf der Hand, dass die Klägerin vor den innerstaatlichen Gerichten weniger benachteiligt gewesen wäre, wenn das Krankenhaus den Zugang zu den Krankenakten stärker kontrolliert hätte, indem es den Zugang auf die unmittelbar an der Behandlung der Klägerin beteiligten Angehörigen der Gesundheitsberufe beschränkt oder ein Protokoll über alle Personen geführt hätte, [...]

[3] Orientierungshilfe Krankenhausinformationssysteme (Version 2), herausgegeben im März 2014 von den Arbeitskreisen „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Online, zitiert am 2021-12-28; verfügbar unter https://lfd.niedersachsen.de/startseite/themen/gesundheit/krankenhaus/orientierungshilfe-krankenhausinformationssysteme-95681.html

[4] Europäischer Gerichtshof für Menschenrechte, Urt. v. 17.07.2008, Application no. 20511/03, Rn. 44. [Online] 2008 [Zitiert 2021-12-28] Verfügbar unter http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf

Im Urteil des EGMR wurde die fehlende Möglichkeit der Feststellung, wer auf die Patientendaten zugegriffen hat, als ein Verstoß gegen Art. 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten[5] beurteilt. Das Urteil des EGMR fordert jedoch nicht explizit eine Protokollierung aller Zugriffe, sondern stellt fest, dass das Recht auf Privatsphäre strenge Kontrollen, Sicherheitsvorkehrungen und den Schutz von Gesundheitsinformationen erfordert, inklusive der Feststellung, wer auf Patientendaten zugegriffen hat. Entsprechend dem Urteil wird eine Protokollierung überall dort erforderlich sein, wo ein Berechtigungskonzept diesen Schutz und die Gewährleistung des Betroffenenrechts hinsichtlich der Auskunft, wer die Daten zur Kenntnis nehmen oder anderweitig verarbeiten konnte, nicht mehr gewährleisten kann. Insbesondere müssen unberechtigte Zugriffe protokolliert werden, so gut es technisch möglich ist.

Letztlich muss ein Verantwortlicher daher zur Erfüllung der oben genannten Anforderungen eine Protokollierung durchführen, sei es dadurch, dass Menschen die Tätigkeit anderer Menschen protokollieren, oder sei es, dass Computersysteme die Zugriffe auf personenbezogene oder personenbeziehbare Daten protokollieren.

Es gibt keinen einheitlichen Aufbau von Protokolldateien, sodass jeder Hersteller von Informationssystemen eine eigene Ansicht bzgl. Inhalt und Aufbau der Protokolldaten hat. Daraus resultiert insbesondere, dass Art, Umfang und Dauer der Protokollierung häufig vom Hersteller des eingesetzten Informationssystems festgelegt werden und die Qualität, mit der Verantwortliche den oben genannten gesetzlichen Anforderungen genügen können, ist von IT-System zu IT-System von sehr unterschiedlicher Güte.

Grundsätzlich ist dabei zu beachten, dass Protokolldateien nahezu immer personenbezogene oder personenbeziehbare Daten beinhalten, z. B. in Form von IP-Adressen, Identifier von Beschäftigten oder Patienten oder auch Angaben zu Zeit und Ort, die einen Rückschluss auf eine Person ermöglichen.

[5] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten – Convention for the Protection of Human Rights and Fundamental Freedoms. Online, zitiert am 2022-01-28; verfügbar unter https://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention

2 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen wurden in der „Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen“[6] dargestellt, sodass an dieser Stelle nur kurz einige ausgewählte Aspekte dargestellt werden.

2.1 Anlassbezogene Kontrolle

Ein konkreter Anlass kann in diesem Zusammenhang nur sein, dass ein Hinweis oder ein Verdacht auf einen unberechtigten Zugriff auf personenbezogene oder personenbeziehbare Daten existiert. In diesen Fällen leitet sich eine Kontrolle der Datenzugriffe unmittelbar aus den Datenschutzgesetzen ab, insbesondere verlangen Artt. 33, 34 DS-GVO die Bereitstellung entsprechender Informationen.

Art. 33 Abs. 5 DS-GVO verlangt die Dokumentation aller Verletzungen des Schutzes personenbezogener Daten, einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten. Aus einer Verletzung des Schutzes personenbezogener Daten resultiert immer auch eine anlassbezogene Überprüfung der Verarbeitung durch den Datenschutzbeauftragten[7], natürlich auch hier verbunden mit der Nutzung der Protokolldaten zur Feststellung und Klärung des Sachverhalts für den entsprechenden Vorfall.[8]

Die Überprüfung selbst kann dabei entsprechend den Empfehlungen des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein im Rahmen eines Stufenmodells erfolgen.[9]

2.2 Anlassunabhängige Kontrolle

Die Erforderlichkeit von anlassunabhängigen Kontrollen durch den Datenschutzbeauftragten ergibt sich aus der in Art. 39 DS-GVO verankerten Prüfpflicht des Datenschutzbeauftragten. Die Häufigkeit der Kontrollen muss entsprechend Art. 39 Abs. 2 DS-GVO „dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung“ tragen, Umfang und Intensität der vom Datenschutzbeauftragten durchgeführten Überprüfungshandlungen muss sich dabei an Umfang und Kritikalität der Datenverarbeitung orientieren.[7]

Die Kontrollen dürfen sich nicht nur auf Bewertungen der Prozessbeschreibungen beschränken, vielmehr umfasst diese Aufgabe stets auch die Überprüfung, ob vorgesehene Sicherheitsmaßnahmen tatsächlich umgesetzt und wirksam sind[10], was immer auch eine Überprüfung und Einsichtnahme in die Unterlagen vor Ort erfordert[11] und damit eine Prüfung der Protokolldaten beinhaltet.

---

[6] „Protokollierung und Protokollierungskonzept – Eine Einführung in die Thematik“, erstellt von den drei verbänden bvitg, GMDS und IHE. Online, zitiert am 2021-12-28; verfügbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php

[7] Drewes S.: Art. 39, Rn. 18, 38-40. In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[8] Lindner M. (2020) Datenschutz und Interne Untersuchungen – mal anders. CCZ: 160-162

[9] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Private sowie dienstliche Internet- und E-Mail-Nutzung, Kapitel 5 „Eskalierendes Stufenmodell“. [Online] 2014 [Zitiert 2021-12-28] Verfügbar unter https://www.datenschutzzentrum.de/artikel/594-Private-sowie-dienstliche-Internet-und-E-Mail-Nutzung.html bzw. pdf-Datei unter https://www.datenschutzzentrum.de/uploads/privatwirtschaft/private-und-dienstliche-internetnutzung.pdf

[10] Bergt M.: Art. 39, Rn. 15. In: Kühling / Buchner (hrsg.) Datenschutz-Grundverordnung / Bundesdatenschutzgesetz: DS-GVO / BDSG. C.H.BECK, 2 Auflage 2018. ISBN 978-3-406-71932-5

[11] Drewes S.: Art. 39, Rn. 19. In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

3 Anforderungen an die Protokollierung

Die aus dem Jahr 2011 bzw. 2014 stammende und auf dem zu diesem Zeitpunkt geltenden „alten“ Datenschutzrecht basierende OH KIS verlangt (Teil 2, Abschnitt 7.1) „eine Protokollierung relevanter Ereignisse“. Diese Ereignisse müssen benannt werden, damit Hersteller von Informationssystemen eine Protokollierung entsprechend anpassen können. Insbesondere unter Berücksichtigung von Art. 5 Abs. 1 lit. c DS-GVO muss eine Protokollierung auf das erforderliche Maß beschränkt werden.

Neben datenschutzrechtlichen Zwecken dienen Protokolldaten regelhaft auch der Fehlersuche im technischen Umfeld. Daher muss vor Beginn der Protokollierung in einem Protokollierungskonzept festgelegt werden, welche Ereignisse zwingend für welchen Zweck für wie lange in einer Protokolldatei verarbeitet/gespeichert werden müssen und wer, unter welchen Bedingungen, wann, auf welche Daten zugreifen darf.

Diese Praxishilfe betrachtet nur den datenschutzrechtlichen Teil, d. h. betrachtet, welche Daten zur Erfüllung der aus dem Datenschutzrecht resultierenden Aufgaben mindestens verarbeitet werden sollten.

3.1 In Normen festgehaltene Anforderungen an eine Protokollierung

3.1.1 Anforderungen aus dem Datenschutz

DIN EN ISO/IEC 27701[12] fordert, dass der Zugriff auf personenbezogene Daten aufzuzeichnen ist, einschließlich Angaben darüber,

- wer,
- wann,
- auf welche personenbezogenen Daten der betroffenen Person zugegriffen hat und
- welche Änderungen (wenn überhaupt) infolge des Ereignisses vorgenommen wurden.

Da entsprechende Protokolle selbst personenbezogene oder personenbeziehbare Daten beinhalten können, müssen Maßnahmen, wie z. B. eine Zugangskontrolle eingeführt werden, um sicherzustellen, dass die protokollierten Informationen nur bestimmungsgemäß genutzt werden.

Ähnlich die ISO/IEC 29101[13]. Die Norm fordert, dass jede Transaktion, die mit personenbezogenen Daten durchgeführt wird, protokolliert wird. Dabei muss die Identität des- oder derjenigen, die auf personenbezogene Daten zugreifen, Transaktionen auf bzw. mit diesen Daten einleiten oder aus diesen Transaktionen resultierende personenbezogene Daten erhalten, im Protokoll festgehalten werden.

Auch die ISO/IEC 29151[14] schreibt eine Protokollierung vor, die insbesondere folgende Informationen beinhalten soll:

- Auf welche personenbezogenen Daten zugegriffen wurde.
- Was (z. B. lesen, drucken, hinzufügen, ändern, löschen) mit den personenbezogenen Daten gemacht wurde.
- Wann dies stattfand.
- Welche Akteure beteiligt waren, d. h. wer mit wessen personenbezogene Daten agierte.

[12] DIN EN ISO/IEC 27701: Sicherheitstechniken – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz – Anforderungen und Leitlinie (Stand: 2021-07). Online, zitiert am 2022-02-05; verfügbar unter https://www.beuth.de/de/norm/din-en-iso-iec-27701/339507443

[13] ISO/IEC 29101: Informationstechnik – Sicherheitstechniken – Architekturrahmenwerk für Datenschutz (Stand: 2018-11). Online, zitiert am 2022-02-05; verfügbar unter https://www.beuth.de/de/norm/iso-iec-29101/299567693

[14] ISO/IEC 29151: Informationstechnik – Sicherheitsverfahren – Leitfaden für den Schutz personenbezogener Daten (Stand: 2017-08). Online, zitiert am 2022-02-05; verfügbar unter https://www.beuth.de/de/norm/iso-iec-29151/278914387

Die Norm schlägt weiterhin vor, dass ein Verfahren zur Überprüfung des Ereignisprotokolls mit einer festgelegten, dokumentierten Periodizität eingeführt werden sollte, um Unregelmäßigkeiten zu erkennen und Abhilfemaßnahmen vorzuschlagen.

3.1.2 Protokollierung in IT-Systemen der Gesundheitsversorgung

Gemäß DIN CEN ISO/TS 14441[15] müssen klinische IT-Systeme in der Lage sein,

- Start und die Beendigung des Systems,
- An- und Abmeldung von Benutzern,
- Benutzerauthentifizierungsversuche und deren Ergebnis (erfolgreich oder nicht erfolgreich),
- Eintrag zur Benutzeridentität,
- Zeitüberschreitungen von Sitzungen,
- Kontosperrungen,
- Sicherung und Wiederherstellung von Informationen,
- Erstellung/Überprüfung einer digitalen Signatur,
- Ereignisse zur Sicherheitsverwaltung, einschließlich Änderungen von Kennwörtern,
- Manipulation von Gesundheitsinformationen, d. h.
    - die Erstellung,
    - den Zugriff auf Informationen,
    - die Änderung,
    - die Löschung sowie
    - den Import, Export, das Ausdrucken oder andere Formen der Weitergabe von persönlichen Gesundheitsinformationen

zu protokollieren. Weiterhin muss bzgl. einer Patientenakte protokolliert werden:

- Erstellung oder Zugriff auf eine Akte einer behandelten Person (z. B. Bildschirmdarstellung, Ausdruck, Download) oder Aktualisierung einer Akte,
- Zugriff auf Daten, die gesperrt oder auf Anweisung eines Patienten/einer Person maskiert sind, mittels eines Notfallzugriffs, inklusive einer Begründung der Notwendigkeit,
- Erstellung und Änderung der Einwilligungserklärungen eines Patienten/einer Person,
- Abfragen von persönlichen Gesundheitsinformationen,
- Import von persönlichen Gesundheitsinformationen (Empfang), einschließlich Datenübertragung und Datenaustausch,
- Export von persönlichen Gesundheitsinformationen, einschließlich Datenübertragung, Datenaustausch und Ausdruck,
- Maßnahmen der Benutzer-, Rollen- und Gruppenverwaltung und
- Aktenvernichtung.

Auch der Zugriff auf die Protokolldateien selbst muss protokolliert werden. Und natürlich müssen für Protokolldateien entsprechende Sicherheitskontrollen eingesetzt werden, um Änderungen und unberechtigten Zugriff zu verhindern.

3.1.3 Protokollierung von Notfallzugriffen

Entsprechend DIN CEN ISO/TS 14441[15] muss der Gebrauch eines Notfallzugriffs immer in einem Protokoll aufgezeichnet werden. Hierbei müssen insbesondere

- die Identität des Benutzers, der mit einem Notfallzugriff auf personenbezogene Daten zugreift,
- der Grund für den Notfallzugriff,
- eine eindeutige Kennung, die zu einem späteren Zeitpunkt zur Identifizierung des Datensubjekts verwendet werden kann,

[15] DIN CEN ISO/TS 14441: Medizinische Informatik – Sicherheits- und Datenschutzanforderungen für die Konformitätsprüfung von EGA-Systemen (Stand: 2014-04). Online, zitiert am 2022-02-05; verfügbar unter https://www.beuth.de/de/technische-regel/din-cen-iso-ts-14441/164574955

- das Datum und
- die Zeit des Notfallzugriffs

protokolliert werden.

3.1.4 Protokollierung bei Langzeitarchivierung

DIN 31644[16] beinhaltet die Forderung, dass bei Langzeitarchivierung Maßnahmen zur Prüfung der Integrität und Authentizität der digitalen Objekte als auch durchgeführte Erhaltungsmaßnahmen wie beispielsweise Dateiformatmigrationen zu protokollieren sind. Hierbei sind entsprechend der Norm insbesondere durch die Protokollierung festzuhalten

- welche Objekte bearbeitet wurden,
- welche Beschäftigten an der Maßnahme beteiligt waren,
- der Grund für die Maßnahme,
- die Berechtigung für die Maßnahme,
- welche technischen Hilfsmittel benutzt wurden,
- der Zeitpunkt,
- die Beschreibung des Vorgangs,
- das geprüfte Ergebnis sowie
- der Ausgang der Aktivität.

3.2 Grundlegende Inhalte der Protokollierung: OH KIS

In Teil 2, Abschnitt 7.10 heißt es in der Orientierungshilfe Krankenhausinformationssysteme (OH KIS) der deutschen Datenschutz-Aufsichtsbehörden:

> *7.10 Neben der Anmeldung am Verfahren (Login/Logout) müssen die Zugriffe der Nutzer mit zumindest folgenden Angaben protokolliert werden:*
>
> - *Zeitpunkt des Zugriffs,*
> - *Kennung des jeweiligen Benutzers,*
> - *Kennung der jeweiligen Arbeitsstation,*
> - *aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung),*
> - *betroffene Patienten/Behandlungsfälle*
>
> *Bei Aufruf einer Suchfunktion muss das Protokoll mindestens enthalten:*
>
> - *verwendete Such- bzw. Abfragekriterien (z. B. Patientennummer, Fallnummer, Name, Geburtsdatum, Wohnort, Diagnose etc.),*
> - *Angaben zum Ergebnis der Abfrage (z. B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske),*
> - *etwaige Folgeaktionen bzw. Navigationsschritte (z. B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).*

Diese Daten erlauben eine Aussage, welche Person zu welchem Zeitpunkt, auf welche Daten und von welcher Arbeitsstation zugegriffen hat. Jedoch reichen diese Angaben ggf. nicht, um zu prüfen, ob der Zugriff auf die personenbezogenen Daten berechtigt war oder nicht.

Beispiel 1: Aushilfe auf anderer Station

Krankenpfleger Paul arbeitet auf Station 23, die zur HNO Klinik gehört. Aufgrund einer Grippewelle ist Station 32, eine Station der internistischen Klinik, unterbesetzt und Krankenpfleger Paul wird für zwei Wochen auf die Station 32 versetzt.

Während dieser Zeitspanne darf Krankenpfleger Paul auf alle Daten der internistischen Patienten der Station 32 zugreifen, aber nicht mehr auf die Patientendaten der Station 23.

[16] DIN 31644: Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive. (Stand: 2012-04). Online, zitiert am 2022-02-05; verfügbar unter https://www.beuth.de/de/norm/din-31644/147058907

Obiges Beispiel ist mit den Vorgaben der Datenschutzbehörden abbildbar: Dadurch, dass die zugreifende Arbeitsstation und damit der Ort, von dem der Zugriff erfolgt im Protokoll festgehalten wird, kann beurteilt werden, ob der zugreifende Arbeitsplatz zum legitimen Arbeitsumfeld wie beispielsweise Arztzimmer, Station oder OP gehört oder nicht. Den Vorschlägen der deutschen Aufsichtsbehörden bzgl. Protokollierung ist daher zuzustimmen, und es müssen zumindest

- der Zeitpunkt des Zugriffs,
- die Kennung des jeweiligen Benutzers sowie Name, Berufsgruppe und Einsatzort
- die Kennung der Arbeitsstation, von welcher auf Patientendaten zugegriffen wird, wobei eine ergänzende Dokumentation die Bestimmung der örtlichen Gegebenheit ermöglichen muss,
- die zugegriffen Datenkategorien wie Stammdaten oder Labordaten sowie
- die Kennungen der vom Zugriff betroffenen Patienten

protokolliert werden.

Beispiel 2: Verlegung eines Patienten

Patient Müller wird vormittags von der operativen Intensivstation auf die chirurgische Station 41 verlegt. Aufgrund der Arbeitsauslastung erfolgt die IT-technische Verlegung, d. h. die Verlegung im Dokumentationssystem, erst am Mittag, wenn sowohl Früh- als auch Spätschicht anwesend ist und genügend Personal für diese Dokumentationsaufgaben zur Verfügung steht. In der Zwischenzeit, d. h. in der Zeitspanne, wo der Patient physisch auf Station 41 liegt, im IT-System aber noch auf der Intensivstation geführt wird, greift das Personal der Station 41 auf die Patientendaten zum Zweck Medikamentengabe zu.

In diesem Beispiel reichen die von der Datenschutzkonferenz angeführten Angaben bzgl. Protokollierung zur Bewertung der Rechtmäßigkeit von Zugriffen nicht aus, denn laut Protokollierung erfolgte der Zugriff auf Patientendaten von einer Arbeitsstation, die nicht zum berechtigten Umfeld gehört. Ein Datenschutzbeauftragter müsste allein aufgrund der Auswertung der Protokolldateien zu dem Schluss kommen, dass ein unberechtigter Zugriff erfolgte.

Damit ein Datenschutzbeauftragter beurteilen kann, ob ein Zugriff rechtmäßig erfolgte oder nicht, muss daher aus der Protokollierung zusätzlich der Kontext, in welchem auf die Patientendaten zugegriffen wurde, ersichtlich sein. In diesen Fällen wird oft von „funktionellen Rollen“ gesprochen.

3.3 Funktionelle und strukturelle Rollen

Im Gesundheitswesen eingesetzte Informationssysteme unterstützen i. d. R. einen rollenbasierten Zugriff, wobei jedem Benutzer eine oder mehrere Rollen zugeordnet werden. Dabei wird jeder Rolle eine oder mehrere Rechte zur Ausübung von durch das Informationssystem bereitgestellte Funktionen, wie beispielsweise das Suchen eines Patienten, zugewiesen. Bei Rollen in Informationssystemen wird zwischen funktionellen und strukturellen Rollen unterschieden (Quelle nachfolgende Begriffsbestimmungen: DIN EN ISO 21298:2017-07[17]):

- **Funktionelle Rollen** sind Rollen, welche an eine Aktivität gebunden sind. Funktionelle Rollen sind beispielsweise „zu betreuende Person“, „behandelnde Ärztin“ oder „verschreibende Person“. In Bezug auf Informationen gehören auch Rollen wie „Verfasser“, „Unterzeichner“ oder „Bereitsteller der Information“ dazu.

[17] DIN EN ISO 21298: Medizinische Informatik - Funktionelle und strukturelle Rollen (Stand: 2017-07). Online, zitiert am 2021-12-28; verfügbar unter https://www.beuth.de/de/norm/din-en-iso-21298/246254631

- **Strukturelle Rollen** sind Rollen, welche Beziehungen zwischen Entitäten im Sinne von Kompetenz festlegen und oftmals organisatorische oder strukturelle Beziehungen (Hierarchien) widerspiegeln. Strukturelle Rollen sind beispielsweise „Abrechnung“, „Arzt“ oder auch „Pflegekraft“.

Die meisten Informationssysteme wie KIS oder PVS bilden strukturelle Rollen ab, funktionale Rollen sind nur in Ausnahmefällen vorgesehen. Dies hat verschiedene Gründe, z. B. müsste für die funktionelle Rolle „behandelnde Ärztin“ nicht nur berücksichtigt werden, welche Ärztin zu welcher Abteilung gehört (was abbildbar wäre), sondern auch, für welche anderen Abteilungen sie im Nachtdienst zuständig ist – was einen Zugriff auf die Personalplanung erfordert. Schnittstellen zu Personalplanungssystemen sind i. d. R. nicht vorhanden, sodass eine doppelte Dokumentation erfolgen müsste, was sehr fehleranfällig wäre und ggf. durch vergessene oder unrichtige Doppeldokumentation zu einer Falschzuordnung führen könnte, sodass im Notfall kein Zugriff auf dringend erforderliche Patientendaten möglich wäre.

Daher stehen in nahezu allen im Gesundheitswesen eingesetzten Informationssystemen nur strukturelle Rollen zur Abbildung der Rechte auf Zugriffe der Informationen zur Verfügung.

3.4 Erfassung des Kontextes von Zugriffen

Was ist mit „Kontext des Zugriffes gemeint? Hierzu ein Beispiel:

Beispiel 3: Bereitschaftsdienst im Krankenhaus

Dr. Musterfrau arbeitet in einem Krankenhaus in der inneren Abteilung. Neben der inneren Abteilung gibt es im Krankenhaus noch eine chirurgische Klinik, eine Klinik für Augenheilbehandlungen und eine gynäkologische Abteilung. Von 7.00 Uhr bis 18.00 Uhr sind alle Kliniken von den jeweiligen Fachärzten besetzt, aber zwischen 18.00 Uhr und 7.00 Uhr sind nur noch ein Facharzt für Chirurgie und ein Facharzt für Innere Medizin im Krankenhaus, die alle Notfälle versorgen.

Dr. Musterfrau darf zwischen 7.00 und 18.00 Uhr nur im Rahmen konsiliarischer Tätigkeiten auf Daten anderer Fachabteilungen wie z. B. der Gynäkologie zugreifen, zwischen 18.00 und 7.00 Uhr auch zur Notfallbehandlung.

Die in der OH KIS benannten Kriterien erlauben keine Aussage, ob eine konsiliarische Tätigkeit oder eine Notfallbehandlung vorlag, die Berechtigung für einen Zugriff auf Patientendaten anderer Fachabteilungen durch Dr. Musterfrau kann daher nicht überprüft werden.

Um die Berechtigung eines Zugriffes zu ermitteln, muss bekannt sein, ob die Ärztin im Beispiel im Rahmen des nächtlichen Bereitschaftsdienstes oder im Kontext ihres normalen Arbeitsbereiches erfolgte. Die Kenntnis dieser Information für die Beurteilung ist unverzichtbar, daher muss diese Information aus der Protokollierung hervorgehen.

4 Protokollauswertungen

Im Rahmen von Anwendungsfällen (sogenannten „Use Cases“) wird beispielhaft beschrieben, welche Anforderungen Datenschutzbeauftragte bei der Erfüllung der in Art. 39 Abs. 1 lit. b DS-GVO verankerten Pflicht zur „Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten“ an die eigene Protokollierung stellen müssen.

Hierzu wird das jeweilige Szenario beschrieben inklusive der Ziele, welche in diesen Szenarien von Datenschutzbeauftragten erreicht werden sollen. Basierend auf diesen Anwendungsfällen wird eine Spezifikation dargestellt, welche den jeweils beschriebenen Use Case in der Praxis abbilden kann.

4.1 Use Cases bzgl. Protokollauswertungen

Im Folgenden werden Szenarien bzgl. Patientendaten beschrieben, aber natürlich werden in einem Krankenhaus neben Patientendaten auch Daten von Beschäftigten verarbeitet, z. B. in HR-Systemen. Die Aufgaben eines Datenschutzbeauftragten beziehen sich grundsätzlich auf alle Verarbeitungen eines Verantwortlichen, in denen Daten betroffener Personen verarbeitet werden. Dementsprechend gelten die nachfolgend beschriebenen Use Cases bzgl. Patientendaten analog für Beschäftigtendaten, d. h. IT-Systeme, mit denen Beschäftigtendaten verarbeitet werden, müssen analogen Anforderungen genügen und entsprechende Auswertungsmöglichkeiten zur Verfügung stellen.

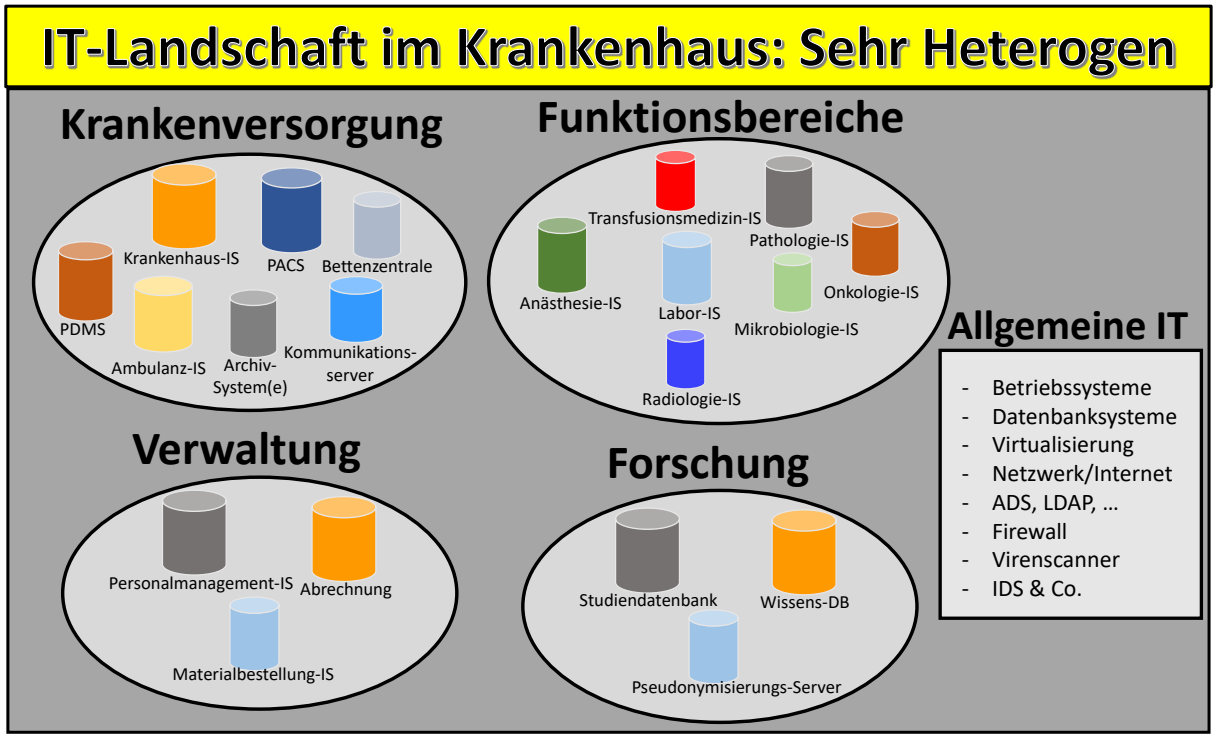

Abbildung 1: In Krankenhäusern vorzufindende IT-Systeme

Abbildung 1 zeigt, wie heterogen die IT-Landschaft in Krankenhäusern sein kann und welche unterschiedlichen IT-Systeme vorhanden sein können. Jedes der IT-Systeme hat einen Fokus auf bestimmte Verarbeitungen bzw. Anwendungen wie beispielsweise die Abrechnung der gegenüber Patienten erbrachten Leistungen. Entsprechend stehen in jedem Informationssystem für sich nur die für die jeweilige Anwendung benötigten Informationen zur Verfügung. So werden Arbeitszeiten in IT-Systemen, die zur Dokumentation von medizinischen Leistungen dienen, eher nicht erfasst, in Systemen zur Personalabrechnung hingegen schon. Letztlich führt dies dazu, dass für

Protokollauswertungen, wie sie in dieser Praxishilfe besprochen werden, Informationen aus unterschiedlichen Informationssystemen zusammengetragen werden müssen.

4.1.1 Anlassabhängige Auswertungen

4.1.1.1 Interne Prüfungen

- **Fall 1:** Verdacht auf unberechtigte Verarbeitung

  Beschreibung Use Case:

  Es besteht der Verdacht, dass bestimmte Beschäftigte unberechtigt Patientendaten verarbeiteten. Der Datenschutzbeauftragte prüft Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Wann griff Beschäftigter 4711 auf Daten von Patient 0815 zu?
  2. Exportierte Beschäftigter 4711 Daten von Patient 0815?
  3. Veränderte Beschäftigter 4711 Daten von Patient 0815?
  4. Zu welchem Zweck erfolgten die in Nr. 1-3 beschriebenen Verarbeitungen durch den Beschäftigten?

  Spezifikation zur Abbildung der Use Cases:

  Im Protokoll des eingesetzten Informationssystems sind folgende Informationen enthalten;

  - Patienten-ID
  - Beschäftigten-ID, Namen, Berufsgruppe und Einsatzort,
  - Datum des Zugriffs
  - Uhrzeit des Zugriffs
  - Art des Zugriffs (= lesend, löschend, ändernd, Ausdruck, externe Speicherung).

  Die Zuordnung des Mitarbeiters zur Beschäftigten ID ist im Informationssystem oder in einem (zentralen) Verzeichnis enthalten. Hierzu muss eine entsprechende Datenbankabfrage erfolgen, welche diese Informationen liefert.

  Aus dem Protokoll können die Patienten ermittelt werden, auf die der Mitarbeiter in einem gewissen Zeitraum zugegriffen hat, sowie Datum und Uhrzeit des Zugriffs.

  Nicht enthalten in einem IT-System ist regelhaft der Grund des Zugriffs. Je nach Berechtigungskonzept[18] müssen weitere Informationen aus dem Informationssystem ermittelt werden. Beispielsweise: Beginn und Ende der Behandlung, Fachabteilung, behandelnde Einheit.

  Für viele Mitarbeiter gibt es Zugriffe, die sich aus ihrer Aufgabenstellung ergeben (siehe auch Berechtigungskonzept) hier kann zunächst von einem berechtigten Zugriff ausgegangen werden.

  Beispiele für berechtigte Zugriffe, die während der Analyse durch den Datenschutzbeauftragten aus vorhandenen Informationen bewertet werden können:

  1. Zugriff erfolgte während der Behandlungsdauer, d. h. im Krankenhaus während der stationären Aufnahme bzw. im ambulanten Umfeld im Kontext eines Patiententermins durch in die Behandlung direkt involvierte Personen wie Ärzte der behandelnden Fachabteilung, Personal der Station, auf welcher der Patient untergebracht ist, oder auch das Personal der niedergelassenen Praxis, wenn die Praxis nur eine medizinische Fachrichtung abbildet.
  2. Zugriff erfolgte zeitnah (2-4 Wochen) nach Entlassung bzw. nach Beendigung durch mit der Abrechnung des Personals betraute Personen und es erfolgten Änderungen und ggf. auch Exporte von Daten, welche die Abrechnung betreffen.
  3. Zugriff erfolgte zeitnah (2-4 Wochen) nach Entlassung bzw. nach Beendigung die in Punkt 1. betrauten Personen, um Behandlungsdaten zu validieren.

[18] Idealerweise gibt es eine systematische Darstellung auf welche Daten oder Patienten ein Mitarbeiter zugreifen darf bzw. welche Daten er wie verarbeiten darf.

4. Zugriff erfolgte im Rahmen eines Konsils. Viele Informationssysteme bieten die Beauftragung eines Konsils in elektronischer Form an, d. h. die Beauftragung erfolgt direkt über das Informationssystem. Über eine Datenbankabfrage kann man feststellen, ob zeitnah vor Datum und Uhrzeit des Zugriffs eine Konsilanfrage an die Fachabteilung erfolgte, zu welcher die zugreifende Person gehört. Liegt eine Konsilanforderung vor, so wird auch von einem berechtigten Zugriff ausgegangen.

In allen anderen Fällen muss die zugreifende Person angesprochen und nach dem Grund gefragt werden, der anschließend auf Richtigkeit überprüft wird.

Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll des Informationssystems, Auswertung der Behandlungsdokumentation, Ergänzend Auswertung von Informationen aus dem Personalmanagementsystem (wann war der Beschäftigte wo eingesetzt) sowie des Berechtigungskonzeptes bzw. Überprüfung des Berechtigungskonzeptes im eingesetzten Informationssystem
2. Protokoll des Informationssystems, Auswertung der Behandlungsdokumentation, Ergänzend Auswertung von Informationen aus dem Personalmanagementsystem (wann war der Beschäftigte wo eingesetzt) sowie des Berechtigungskonzeptes bzw. Überprüfung des Berechtigungskonzeptes im eingesetzten Informationssystem
3. Protokoll des Informationssystems, Auswertung der Behandlungsdokumentation, Ergänzend Auswertung von Informationen aus dem Personalmanagementsystem (wann war der Beschäftigte wo eingesetzt) sowie des Berechtigungskonzeptes bzw. Überprüfung des Berechtigungskonzeptes im eingesetzten Informationssystem
4. Bei Notfall- oder Sonderzugriffen: Protokoll des Informationssystems

- **Fall 2:** Weitergehende Rechte, als zugeordnete Rollen beinhalten

  Beschreibung Use Case:

  Zur Bearbeitung bestimmter Aufgaben müssen zeitweise an Beschäftigte weitergehende Rechte übertragen werden, als diese entsprechend Berechtigungskonzept bekommen sollten. Dies kann z. B. aufgrund von Vertretungen erkrankter oder im Urlaub befindlicher Personen der Fall sein. Diese Rechte sind nur für die Zeitdauer dieser speziellen Tätigkeit erforderlich, müssen anschließend wieder entfernt werden. Der Datenschutzbeauftragte prüft Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Wurden Beschäftigten zusätzliche Rechte übertragen?
  2. Waren diese Rechte für die Tätigkeiten der Beschäftigten erforderlich?
  3. Wurde die Erweiterung der Rechte von einer zeichnungsberechtigten Person veranlasst?
  4. Wurden die Rechte nach Beendigung der Tätigkeit wieder entfernt?

  Spezifikation zur Abbildung der Use Cases:

  Die Benutzer- und Berechtigungsverwaltung sollte eine Änderungshistorie führen (Protokollierung). Aus dieser ist ersichtlich, ob und wie Rechte vergeben wurden.

  Die Metaebene, warum ein Mitarbeiter bestimmte Rechte erhält, sollte durch ein Vorgangsbearbeitungssystem zur Beantragung unterstützt werden. Aus der Vorgangsbearbeitung ergibt sich, dass nur berechtigte Personen die Zuweisung von Rechten bestätigen dürfen, der Vorgang ist nachvollziehbar dokumentiert.

  Vorgangsbearbeitungssystem für die Verwaltung der Benutzerrechte sind teilweise in Identity Management Systemen und in Systemen zur Unterstützung von Governance und Compliance integriert. Unterstützt das zentrale System das Anlegen, Ändern und Stornieren von Berechtigungen ist die Dokumentation in der Benutzer- und Berechtigungsverwaltung manchmal

nur begrenzt aussagefähig, sodass dann die ganze Prüfung in dem zentralen System erfolgen sollte.
AdHoc Lösungen über E-Mail sind nur begrenzt auswertbar bzw. es ist bei der SOP darauf zu achten, dass alle nötigen Informationen an Stellen abgelegt werden, die von dem Datenschutzbeauftragten oder Auditoren eingesehen werden können.
Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll der Benutzer- und Berechtigungsverwaltung im eingesetzten Informationssystem
2. Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem
3. Protokoll Identity Managementsystem (wenn so etwas eingesetzt wird) alternativ Governance, Risk and Compliance System oder „Papierdokumentation“
4. Protokoll der Benutzer- und Berechtigungsverwaltung im eingesetzten Informationssystem

4.1.1.2 Betroffene Person fordert Prüfung bzgl. Datenzugriffe

- **Fall 1:** Zugriff auf Patientendaten nach Entlassung

  Beschreibung Use Case:
  Aufnahmekraft greift 14 Tage nach der Entlassung eines Notfall-Patienten auf Daten desselben zu. Das Protokoll listet nicht auf, auf welche Daten zugegriffen wurde. Der betroffene Patient beschwert sich, dass ein aus seiner Sicht unberechtigter Zugriff erfolgte und verlangt vom Verantwortlichen eine Prüfung und Auskunft nach Art. 15 DS-GVO. Die Aufnahmekraft kann sich an den Vorgang nicht mehr erinnern und nennt die üblichen Gründe, zu welchen Zwecken nach Entlassung eines Patienten ein Zugriff notwendig war, wie Nachfrage eines Kostenträgers, eines Nachbehandlers etc. (diese Aufgaben sind hier organisatorisch der Aufnahme zugeordnet). Der Datenschutzbeauftragte prüft Protokolle.
  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Wann griff Person 4711 auf Daten von Patient 0815 zu?
  2. Aus welchen Gründen griff Person 4711 zum Zeitpunkt tt.mm.jjjj hh.mm auf Daten von Patient 0815

  Spezifikation zur Abbildung der Use Cases:
  Der Zugriff des Mitarbeiters auf den Patienten bzw. seine Daten ist in dem Basisprotokoll des Informationssystems enthalten.
  Um einen mutmaßlichen Zweck des Zugriffs zu ermitteln, könnte eine umfangreiche Protokollierung etabliert und interpretiert werden. Ggf. kann auch aus einem existierenden oder vor kurzem abgeschlossenen Behandlungsfall auf einen rechtmäßigen Zugriff rückgeschlossen werden.
  Je nach Architektur des Informationssystems können zusätzliche Ereignisse wie die ausgeführten Funktionen (z. B. Aufruf der Diagnosen Dokumentation) protokolliert werden. In modernen Architekturen haben medizinische Informationsobjekte (z. B. Dokumente, Diagnosen, Verordnung von Medikamenten) eindeutige IDs, die auch für die Protokollierung des Zugriffs genutzt werden können. Umgekehrt unterstützen moderne Architekturen zunehmend „intelligente“ Übersichten, hier wird eine differenzierte Protokollierung von Informationsobjekten sehr aufwändig.
  Die maximale Forderung wäre die Protokollierung aller gezeigten Daten. Diese maximale Forderung verbraucht viele Ressourcen und ist nur mit großem Aufwand zu interpretieren.
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll des Informationssystems

2. Protokoll des Informationssystems, ergänzend ggf. Auswertung der Abrechnungsdaten im KIS

- **Fall 2:** Anfrage Patient, ob Sperrung beachtet wurde

  Beschreibung Use Case:

  Patient verlangt Sperrung seiner Akte. Zwei Jahre später fragt der Patient beim Datenschutzbeauftragten nach, ob und, wenn ja, aus welchen Gründen von wem die Sperrung aufgehoben wurde. Der Datenschutzbeauftragte prüft Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Sind die Daten von Patient 0815 gesperrt?
  2. Seit wann sind die Daten von Patient 0815 gesperrt?
  3. Wurde die Sperrung der Daten von Patient 0815 im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm aufgehoben?
  4. Wenn die Sperrung aufgehoben wurde: Wer hat dies wann aus welchen Gründen veranlasst?
  5. Wann und wer hat auf Daten von Patient 0815 zugegriffen?
  6. Was waren die Gründe für die Zugriffe nach Aufhebung der Sperrung?

  Spezifikation zur Abbildung der Use Cases:

  Der Use Case setzt voraus, dass es eine Funktion zum Sperren und Entsperren von Patienten bzw. Patientendaten gibt. Typischerweise wird das durch ein Kennzeichen zum Patienten verwaltet. Für dieses Kennzeichen sollte es eine Änderungshistorie geben. Aus dieser kann ermittelt werden, wann das Sperrkennzeichen gesetzt und wieder aufgehoben wurde. Aus diesem Protokoll ist auch ersichtlich, wer ggf. die Sperre aufgehoben hat (Mitarbeiter ID müsste bei Bedarf wieder über die Benutzerverwaltung in identifizierende Informationen übersetzt werden.)

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Sperrkennzeichen im Informationssystem; ggf. Abfrage per Bericht
  2. Protokoll im eingesetzten Informationssystem
     konkret Änderungsprotokoll zum Sperrkennzeichen
  3. Protokoll im eingesetzten Informationssystem
     konkret Änderungsprotokoll zum Sperrkennzeichen
  4. Dies muss in der Patientenakte oder in begleitenden Dokumenten dokumentiert und damit ausgewertet werden.
  5. Protokoll im eingesetzten Informationssystem
     Sonderfall von Fall 3
  6. Protokoll Informationssystem

- **Fall 3:** Beschäftigte fragt nach, wer ihre als Patientin angefallenen Daten verarbeitete

  Beschreibung Use Case:

  Beschäftigte des Klinikums fragt nach, wer, aus welchen Gründen, auf die Daten ihrer medizinischen Behandlung im Klinikum Zugriff nahm. Der Datenschutzbeauftragte prüft die Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen haben entsprechend Berechtigungskonzept das Recht auf einen Zugriff auf Daten von Patient 0815?
  2. Aus welchen Gründen haben diese Personen Zugriff auf Daten von Patient 0815?
  3. Welche Personen griffen zu welchen Zeitpunkten auf Daten von Patient 0815 zu?

4. Aus welchen Gründen griffen diese Personen zu diesen Zeitpunkten auf Daten von Patient 0815 zu?

Spezifikation zur Abbildung der Use Cases:
Das Protokoll des Informationssystems liefert den Zusammenhang, welcher Mitarbeiter (ID) zu welchem Zeitpunkt (Datum, Uhrzeit) auf die Akte des Patienten (ID) mit welcher Aktion (schreibend, lesend, …) zugegriffen hat.
Aus der Patientenverwaltung lässt sich einfach die Patienten ID und wenn nötig eine Fall ID des betroffenen Patienten ermitteln.
Zur Mitarbeiter ID kann in der Benutzerverwaltung identifizierende Informationen wie Name des Mitarbeiters ermittelt werden.
Bei Regelzugriffen wird es praktisch nicht möglich sein, die Gründe zu dokumentieren. Hier müsste auch die Unschuldsvermutung gelten. Offen bleiben der Aufwand und die Strategie, wie man aus den Kontextinformationen wie Rechte und Rollen, Uhrzeit/Regelarbeitszeit, Dienstplan, etc. Routinezugriffe von unberechtigten abgrenzen kann.
Aus dem Berechtigungskonzept können die Rollen entnommen werden, die wahrscheinlich einen Regelzugriff im Rahmen ihrer Aufgaben vollzogen haben. Über die Benutzerverwaltung kann abgeklärt werden, ob den Mitarbeitern, die zugegriffen haben, eine dieser Rollen zugeordnet ist.
Bei Sonderzugriffen kann entweder die Klasse wie Notfall ins Protokoll aufgenommen und ausgewertet werden oder es gibt eine Protokollierung des Grundes für spezielle Sonderzugriffe.
Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll des Informationssystems
   Berechtigungskonzept
2. (Protokoll Informationssystem)
   Ggf. Berechtigungskonzept, Rolle des Benutzers, Organigramm
3. Protokoll des Informationssystems
4. Berechtigungskonzept bei Regelzugriffen
   eventuell sind Zugriffe nach der Behandlung genauer zu prüfen, weil die Anzahl berechtigter Zugriff und berechtigter Personen nach der Entlassung abnehmen sollte
   Protokoll der Begründungen bei Sonderzugriffen im eingesetzten Informationssystem, d. h. es erfolgt eine Dokumentation bei Nutzung von Sonderzugriffen im eingesetzten Informationssystem

- **Fall 3a:** Beschäftigte fragt nach, wer ihre als Patientin angefallenen Daten verarbeitete
  Beschreibung Use Case:
  Nach einer problematischen Geburtssituation einer Mitarbeiterin (Kind stirbt) vermutet die Beschäftigte, dass mehrere Beschäftigte des Hauses lesend und schreibend auf die Dokumentation zugegriffen haben und beauftragt den Datenschutzbeauftragten mit einer Prüfung. Der Datenschutzbeauftragte prüft daraufhin die Protokolle.
  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:
  1. Welche Personen griffen auf die Daten Patient 0815 (Beschäftigte der Klinik bzw. Kind) im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griffen die Personen im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm jeweils auf die Daten Patient 0815 zu?

  Spezifikation zur Abbildung der Use Cases:
  Aufgrund einer speziellen Situation kann vielleicht mehr Kontextinformation ermittelt werden.
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):
  1. Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Ggf. Berechtigungskonzept, Rolle des Benutzers, Organigramm

- **Fall 4:** Patient fordert Auskunft, ob seine Daten gelöscht wurden

  Beschreibung Use Case:

  Patient forderte die Löschung seiner Daten. Ein Jahr später fragt er beim Datenschutzbeauftragten an, ob all seine Daten gelöscht wurden oder ob die Klinik noch Daten über ihn gespeichert hat und wenn ja, welche, aus welchen Gründen, aufgrund welcher Rechtsgrundlage. Der Datenschutzbeauftragte prüft die Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Liegen Informationen zu Patient 0815 im Informationssystem vor?
  2. Wenn ja: Welche Informationen sind im Informationssystem gespeichert?
  3. Aus welchen Gründen wurden diese Daten trotz Löschanfrage des Patienten 0815 nicht gelöscht?
  4. Wurde der Patient 0815 über die nicht erfolgte Löschung sowie der Gründe informiert?

  Spezifikation zur Abbildung der Use Cases:

  Ob zu einem Patienten Daten im Informationssystem vorhanden sind, lässt sich am einfachsten beantworten, wenn der Patient noch einen Eintrag im Verzeichnis der Patienten hat (Patientenstammdaten). Dann kann ermittelt werden, ob unter der entsprechenden ID typische patientenbezogene Informationen gespeichert sind.

  Eigentlich sollte das Verzeichnis der Verarbeitungstätigkeiten alle Verfahren aufführen, in denen weiter Patientendaten gespeichert sein könnten. Damit könnten weitere Informationssystem (mit ggf. abweichenden Aufbewahrungsfristen wie PACS) identifiziert und in die Analyse einbezogen werden.

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Abfrage des Informationssystems
  2. Abfrage des Informationssystems
  3. Metadaten, die in einem speziellen System dokumentiert werden sollten (wenn vorhanden). Dokumentation im eingesetzten Informationssystem, Abfrage im eingesetzten Informationssystem
  4. Metadaten, die in einem speziellen System dokumentiert werden sollten (wenn vorhanden). Dokumentation im eingesetzten Informationssystem, Abfrage im eingesetzten Informationssystem

- **Fall 5:** Patient (VIP) fragt nach, wer auf Daten zugegriffen hat

  Beschreibung Use Case:

  VIP war zur Behandlung im Krankenhaus. Aus gegebenem Anlass (Nachfrage VIP oder weil vorher schon einmal eine Beschwerde einging oder die Krankenhausleitung nachfragte oder …) überprüft der DSB nach der Entlassung des VIP, welche Personen, aus welchen Gründen auf die Daten des VIP zugriffen. Der Datenschutzbeauftragte prüft die Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen griffen auf die Daten Patient 0815 (VIP) im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griffen die Personen im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm jeweils auf die Daten Patient 0815 zu?

  Spezifikation zur Abbildung der Use Cases:

  Technisch läuft dieser Use Case auf Fall 3 hinaus. Auch wenn vielleicht das Krankenhaus aus eigener Veranlassung eine Stichprobe von VIPs prüfen würde (siehe auch 4.1.2 Fall 1).

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll im eingesetzten Informationssystem
2. Protokoll im eingesetzten Informationssystem
3. Ggf. Berechtigungskonzept, Rolle des Benutzers, Organigramm

4.1.1.3 Datenschutz-Aufsichtsbehörde verlangt Auskunft

- **Fall 1:** Datenschutz-Aufsichtsbehörde erkundigt sich wegen potenziellen Datenschutz-Vorfalls

  Beschreibung Use Case:

  Ein Mitarbeiter loggt sich in das Krankenhausinformationssystem (KIS) ein. An diesem Tag und in dieser Abteilung kommt es zu einem gravierenden medizinischen Vorfall, der kurze Zeit später in der Lokalpresse thematisiert wird. Offenbar nutzen diverse andere Mitarbeitende den Login des besagten Mitarbeiters. Wo wird außer im KIS noch protokolliert? Die Datenschutz-Aufsichtsbehörde erkundigt sich nach möglichen Datenabflüssen. Der Datenschutzbeauftragte prüft die Protokolle.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen griffen auf Patientendaten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griffen diese Personen auf Patientendaten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  3. Welche dieser Personen exportierte Patientendaten?
  4. Aus welchen Gründen erfolgte der Export von Patientendaten?

  Spezifikation zur Abbildung der Use Cases:

  In der Regel nutzen die Informationssysteme die erfassten Informationen für die Protokollierung, d. h. als Benutzer wird der angemeldete Benutzer protokolliert unabhängig davon, ob er oder an anderer an er Tastatur sitzt.

  Um aussagefähige Protokolle zu erhalten, sind entsprechende organisatorische Maßnahmen zu treffen und ggf. zu überwachen (einfache Bereitstellung eines individuellen Arbeitsplatzes und Überprüfung z. B. durch Auswertung der Logindaten).

  Ein individueller Export von Patientendaten durch Drucken oder Download sollte über die Protokollierung der Aktionen möglich sein.

  Ein technischer Export sollte über die Einrichtungsdaten der Kommunikationsdienste ermittelt werden. Diese sind auch entsprechend in ihrer Änderung zu protokollieren.

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Protokoll im eingesetzten Informationssystem
  4. Protokoll im eingesetzten Informationssystem durch explizite Abfragen); ggf. ist auch eine externe Dokumentation erforderlich, wenn das Informationssystem keine Möglichkeit bietet, entsprechende Informationen zu erfassen

- **Fall 2:** Datenschutz-Aufsichtsbehörde auditiert Gesundheitseinrichtung

  Beschreibung Use Case:

  Die Datenschutz-Aufsichtsbehörde verlangt im Rahmen eines allgemeinen Audits die Darstellung, ob und welche Auswertungen möglich sind. Der Datenschutzbeauftragte prüft Protokolle im Beisein der Aufsichtsbehörde und zeigt exemplarisch:

  1. Darstellung Zugriffe auf Patient 0815: Auswertung aller Mitarbeiter inkl. Darstellung, welchen Zwecken diese Zugriffe dienten und weshalb diese Zugriffe entsprechend Berechtigungskonzept legitim waren

2. Darstellung der Zugriffe eines zufällig ausgewählten Beschäftigten: Auswertung der Zugriffe auf alle Patienten inkl. Darstellung, welchen Zwecken diese Zugriffe erfolgten und weshalb diese Zugriffe entsprechend Berechtigungskonzept legitim waren
3. Darstellung der Überprüfung, welche Rechte welcher Beschäftigten wann verändert wurden

Spezifikation zur Abbildung der Use Cases:

Fragen 1 und 2 lassen sich mit den bereits beschriebenen Use Cases beantworten.
Die Überprüfung, welche Zugriffsrechte für die Mitarbeiter geändert wurden, wem zusätzlich Rechte gewährt und wieder entzogen wurden, kann in der Regel über die Benutzer und Berechtigungsverwaltung dargestellt werden (siehe 4.11. Fall 2). Wird bei der Berechtigungsverwaltung mit Profilen und Generatoren gearbeitet, kann es sein, dass die Darstellung zusätzlich aufbereitet werden muss.
Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll im eingesetzten Informationssystem
   Abgleich Berechtigungskonzept und vorhandene Rechte im eingesetzten Informationssystem
2. Protokoll Informationssystem
   Abgleich Berechtigungskonzept und vorhandene Rechte im eingesetzten Informationssystem
3. Protokoll der Benutzer- und Berechtigungsverwaltung im eingesetzten Informationssystem

4.1.2 Stichprobenartige Auswertungen (anlassunabhängig)

- **Fall 1:** Prüfung, wer auf Protokolldaten zugegriffen hat

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, wer auf Protokolldateien wann und zu welchen Zwecken zugegriffen hat. Hierzu müssen die Aufzeichnungen folgende Informationen zur Verfügung stellen oder die auf andere Weise bereitgestellt werden müssen:

  1. Wer hat auf die Daten zugegriffen?
  2. Wann wurde auf die Daten von Person 0815 auf die Daten zugegriffen?
  3. Zu welchen Zwecken erfolgte zum Zeitpunkt tt.mm.jjjj hh.mm von Person 0815 Zugriff auf die Daten?
  4. Ist die Person berechtigt gewesen auf die Daten zuzugreifen?

  Spezifikation zur Abbildung der Use Cases:

  Typischerweise werden Protokolleinträge ebenfalls als personenbezogene Daten betrachtet und der Zugriff wird über Berechtigungen geschützt.
  Da es keine Use Cases gibt, in denen zeitkritisch auf Protokolldaten zugegriffen werden muss, kann man den Zugriff sehr gut auf die Berechtigten einschränken. Im Zweifel kann dieser Kreis auch stärker beschränkt werden, bei Bedarf kann der Kreis erweitert werden oder die Analyse der Protokolle wird in einer Gruppe vorgenommen, von der nur einer die Berechtigung im System braucht.
  Die Analysen sollten protokolliert werden (organisatorische Regelung).
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Rechteverwaltung im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Metadaten, die in einem speziellen System dokumentiert werden sollten (wenn vorhanden). Dokumentation im eingesetzten Informationssystem

4. Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem, Schichtplan des Zeitpunktes

- **Fall 2:** Prüfung bei zufällig ausgewählten Patienten, ob Exporte von ihren Daten rechtmäßig erfolgten

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte bei zufällig ausgewählten Patienten, welche Exporte von Patientendaten aus welchen Gründen, durch welche Mitarbeiter, zu welchen Zeitpunkten erfolgt sind. Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Arten von Exporten existieren und welche konkreten Exporte haben stattgefunden?
  2. Wer exportierte welche Daten?
  3. Wann erfolgte durch Person 4711 ein Export dieser Daten?
  4. Zu welchen Zwecken erfolgte zum Zeitpunkt tt.mm.jjjj hh.mm von Person 4711 ein Export dieser Daten?
  5. Gab es eine datenschutzrechtliche (Rechts-) Grundlage für den Export?
  6. Ist die Person berechtigt gewesen die Daten zu exportieren?

  Spezifikation zur Abbildung der Use Cases:

  Grundsätzlich gibt es verschiedene Exportwege, die unterschiedliche Protokollierungen bedienen:

  - Patienten bezogene Ad-hoc Exporte wie: Ausdruck der Krankenakte, Kopie von Bildern auf eine CD, Füllen der ePA. Dies sollte als Patientenbezogene Funktion im Informationssystem protokolliert werden. Export, Ausdruck, Kopie auf CD sollte analog den Dialogzugriffen geprüft werden.
  - Routine Datenübertragung von Patientendaten zu einem gewissen Zeitpunkt nach definierten (parametrierten) Regeln. Dies sollte bei der Einrichtung eines solchen Dienstes dokumentiert werden. Gut wäre ein zentrales Verzeichnis oder ein Konzept.
  - Routine Datenübertragung von Patientenmengen (Beispiele: Qualitätssicherung, Register, Übertragung in ein BI System, Übertragung ins Archivsystem, Kopie von Aktenauszügen für BCM). Die Erstellung der zu übertragenden Datei wird protokolliert, der Inhalt ergibt sich oft nur aus der Kopie bzw. der Verfahrensbeschreibung und den „Selektionskriterien“.
  - Statistische Auswertungen sollten ein anonymisiertes Ergebnis haben. Exporte zu Forschungszwecken sollten durch organisatorische Regelungen und ggf. ihren Antrag dokumentiert sein.

  Die (Routine-)Exporte, die keine „Kopie“ von Patientendaten zur Übermittlung an den Patienten oder Weiterbehandelnde sind, sollten in dem Verzeichnis der Verfahren aufgeführt sein und darüber ihre Rechtmäßigkeit dokumentieren.

  Entsprechend differenziert müssten sich die Berechtigungen erteilen lassen.

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Verfahrensbeschreibung,
     Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Protokoll im eingesetzten Informationssystem
  4. Protokoll im eingesetzten Informationssystem
  5. Bewertung durch den DSB

6. Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem, Protokoll im eingesetzten Informationssystem (Sondererlaubnis?), Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem, Schichtplan des Zeitpunktes

- **Fall 3:** Prüfung bei zufällig ausgewählten Beschäftigten, ob durch sie durchgeführte Exporte von Patientendaten rechtmäßig erfolgten

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche Exporte von Patientendaten aus welchen Gründen, durch welche Mitarbeiter, zu welchen Zeitpunkten erfolgt sind.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Exportwege existieren?
  2. Wer exportierte welche Patientendaten?
  3. Wann erfolgte durch Person 4711 ein Export dieser Patientendaten?
  4. Zu welchen Zwecken erfolgte zum Zeitpunkt tt.mm.jjjj hh.mm von Person 4711 ein Export dieser Patientendaten?
  5. Wurde der Betriebs- / Personalrat oder Mitarbeitervertretung mit einbezogen?
  6. War die Person 4711 dazu berechtigt?

  Spezifikation zur Abbildung der Use Cases:

  Für den Umgang mit den Protokolldaten sollte es ein Konzept geben, in der Regel wird ein Export von Protokolldaten im Rahmen der IT-Sicherheit Maßnahmen angestoßen.

  Für die Analyse, welche Exporte von Protokolldaten ein Mitarbeiter vorgenommen hat, müsste die Anwendung zur Verwaltung der Protokolldaten das Ausführen der Funktionen protokollieren. Bei vielen Anwendungen steht der Schutz der „fachlichen“ Daten (z. B. Patientendaten bei EHR, Personaldaten bei HR) im Vordergrund und deshalb gibt es zwar einen Zugriffschutz und die Kontrolle von Änderungen für die Protokolldaten aber selten eine Protokollierung der Zugriffe auf ein Protokoll.

  Damit bleiben ggf. nur die Aufzeichnungen der Mitarbeiter im Rahmen von ITIL Maßnahmen oder aufgrund organisatorischer Anweisungen. Man könnte dies in einem Vorgangsbearbeitungssystem dokumentieren. (Im Rahmen von ITIL oder IT-Sicherheit)

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Verfahrensbeschreibung
  2. Protokoll im eingesetzten Informationssystem
  3. Protokoll im eingesetzten Informationssystem
  4. Protokoll im eingesetzten Informationssystem
  5. Rücksprache mit Abteilung
  6. Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem, Protokoll im eingesetzten Informationssystem (Sondererlaubnis?), Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem, Schichtplan des Zeitpunktes

- **Fall 4:** Prüfung der Einhaltung von Löschvorgaben

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, ob Löschzyklen eingehalten wurden oder Daten unrechtmäßig länger gespeichert wurden.

  Hierzu müssen die Löschprotokolle folgende Informationen beinhalten:

  1. Wann wurde gelöscht? (Datum/Uhrzeit)

2. Wer veranlasste die Löschung, ist also Verantwortlicher für die Löschung?
3. Wer führte die Löschung durch?
4. Wie erfolgte die Löschung? (Methode des Löschvorgangs)
5. Beschreibung der zu löschenden Daten, Datenarten/-kategorien
6. Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport);
7. Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport)
8. Hinterlegte Löschfristen

Weiterhin muss im KIS festgestellt werden, welche Daten vorhanden sind, obwohl sie hätten gelöscht werden sollen.
Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten können oder die auf andere Weise bereitgestellt werden müssen:

9. Welche Daten im IT-System sind noch vorhanden, obwohl die Daten entsprechend Löschkonzept gelöscht sein müssten?
10. Gab es eine Löschaufforderung?
11. Wer veranlasste, dass die Daten nicht gelöscht wurden?
12. Was sind die Gründe dafür, dass die Daten weiterhin gespeichert werden?
13. Hinterlegte Löschfristen

Spezifikation zur Abbildung der Use Cases:
In diesem Fall geht es um die Löschung von Patientendaten mit Hilfe von Programmen, die ausgewählte Entitäten und ihre Daten löschen. Dies wird idealerweise protokolliert. Ein Löschen einzelner Informationen wie das Löschen der Diagnosen, die zu einem Fall irrtümlich dokumentiert wurden, ist eine Änderung der Patientendaten bzw. Krankenakte und wird als Bearbeitung protokolliert.
Wenn als Löschmethode die Ausführung eines Programmes gewählt wurde, könnte die Beschreibung der zu löschenden Daten in der Programm Dokumentation stehen. Das Programm sollte dann die Steuergrößen, die variabel sind, wie Selektionsparameter oder Löschfrist in das Protokoll übernehmen.
Für die Beantwortung des zweiten Teils der Fragen kann man davon ausgehen, dass die Löschprogramme entsprechend ihrer Spezifikation korrekt arbeiten und Daten nicht gelöscht werden, wenn beispielsweise zusätzliche Informationen wie ein Sperrkennzeichen oder bestimmte Metainformationen vorhanden sind.
Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Löschprotokoll
2. Löschprotokoll
3. Löschprotokoll
4. Löschprotokoll
5. Löschprotokoll
6. Löschprotokoll
7. Löschprotokoll
8. Abgleich Löschkonzept und dessen Umsetzung im eingesetzten Informationssystem
9. Auswertung im Informationssystem
10. Protokoll im eingesetzten Informationssystem, Metasystem zur Verwaltung von Löschanträgen (wenn vorhanden)
11. Protokoll im eingesetzten Informationssystem, Metasystem zur Verwaltung von Löschanträgen (wenn vorhanden)
12. Protokoll im eingesetzten Informationssystem, Metasystem zur Verwaltung von Löschanträgen (wenn vorhanden)
13. Abgleich Löschkonzept und dessen Umsetzung im eingesetzten Informationssystem

- **Fall 5:** Stichprobenartige Kontrolle von Beschäftigten, ob diese berechtigt auf Patientendaten zugreifen

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, auf welche Patienten zufällig ausgewählter Beschäftigter (user) in einer definierten Periode zugegriffen hat.
  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Auf welche Patientendaten griff user 4711 im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griff user 4711 im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm auf diese Patientendaten zu?
  3. War user 4711 hierzu berechtigt?

  Spezifikation zur Abbildung der Use Cases:

  Entspricht technisch dem Fall 1
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Berechtigungskonzept sowie dessen Umsetzung im eingesetzten Informationssystem, Schichtplan

- **Fall 6:** Stichprobenartige Kontrolle, ob Zugriffe auf zufällig ausgewählte Patienten rechtmäßig erfolgten

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche Beschäftigten in einer definierten Periode auf einen zufällig ausgewählten Patienten zugegriffen haben.
  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen griffen auf die Daten von Patient 0815 im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griffen die Beschäftigten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm jeweils auf die Daten von Patient 0815 zu?
  3. Waren die Personen hierzu berechtigt?

  Spezifikation zur Abbildung der Use Cases:

  Entspricht technisch dem Fall 3 für einen frei zu bestimmenden Patienten
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem
  3. Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem

- **Fall 7:** Stichprobenartige Kontrolle von Zugriff auf „VIP“

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche Beschäftigten in einer definierten Periode auf als VIP gekennzeichnete Patienten zugegriffen haben.
  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

1. Welche Personen griffen auf die Daten von als VIP gekennzeichneten Patienten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
2. Aus welchen Gründen griffen die Beschäftigten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm jeweils auf die Daten von den als VIP gekennzeichneten Patienten zu?
3. Waren die Personen hierzu berechtigt?

Spezifikation zur Abbildung der Use Cases:

Entspricht technisch dem Fall 6, wobei bei beim „Ziehen" der Patienten ein Patient mit VIP Kennzeichen gewählt werden muss.

Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll im eingesetzten Informationssystem
2. Protokoll im eingesetzten Informationssystem
3. Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem

- **Fall 8:** Stichprobenartige Kontrolle der Nutzung von „Sonderzugriffen"

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, die Nutzung von „Sonderzugriffen", d. h. wer hat mit der Notfallberechtigung auf welche Patienten zu welchen Zeitpunkten aus welchen Gründen zugegriffen.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen griffen mit folgenden Sonderrechten
     a. Notfallberechtigung
     b. Qualitätssicherung
     c. Forschung/klinische Studie
     d. Auskunft (nach eingesetzter Sperrung)
     e. …

     auf die Daten von Patienten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm zu?
  2. Aus welchen Gründen griffen die Beschäftigten im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm mit Sonderrechten auf die Daten von Patienten zu?
  3. Waren die Sonderzugriffe notwendig?
  4. Gehört der Beschäftigte zu den für Sonderzugriffe Berechtigten?

  Spezifikation zur Abbildung der Use Cases:

  Dieser Fall geht davon aus, dass Sonderzugriffe im Informationssystem erkannt werden können bzw. aktiv ausgelöst werden müssen. Beispiel sind:

  - es gibt eine Rolle, die der Benutzer übernimmt, und dieser Wechsel kann protokolliert werden, ebenso wie die folgenden unter dieser Rolle ausgeführten Aktionen
  - das System kann erkennen, dass der Benutzer zusätzliche Rechte braucht und bietet über einen Popup an, dass der Benutzer einen bestimmten Kontext mit zusätzlichen Rechten ausführen darf[19].

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem, Dokumentation der Sonderzugriffe
  3. Protokoll im eingesetzten Informationssystem, Dokumentation des Verarbeitungsvorgangs im, ggf. auch außerhalb des Informationssystems - Plausibilitätsprüfung, Dokumentation der Sonderzugriffe im eingesetzten Informationssystem

[19] Viele Betriebssystem kenn die Funktion „ausführen als …" mit zusätzlichen Administratorenrechten

4. Protokoll im eingesetzten Informationssystem, Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem

- **Fall 09:** Stichprobenartige Kontrolle der Zugriffe Externer

  Beschreibung Use Case:

  Es erfolgen im Krankenhaus Zugriffe von außerhalb des eigenen Systems auf Patientendaten, z. B. durch eine externe Kodierfachkraft oder durch den MDK, dem man einen eigenen Zugang bereitstellte. Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche externen Zugriffe auf welche Patientendaten, aus welchen Gründen erfolgte.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen griffen von extern im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm auf welche Patientendaten zu?
  2. Aus welchen Gründen griffen diese Personen von extern im Zeitraum von tt.mm.jjjj hh.mm bis tt.mm.jjjj hh.mm auf welche Patientendaten zu?
  3. Waren diese Personen hierzu berechtigt?

  Spezifikation zur Abbildung der Use Cases:

  Um die Zugriffe Externer prüfen zu können, müssen die Externen entsprechende Benutzerkennungen erhalten. Wenn es organisatorisch sinnvoller ist mehrere Externe auf einer Kennung arbeiten zu lassen, muss in einer Zusatzdokumentation festgehalten werden, wer zu einem Zeitpunkt mit der Kennung gearbeitet hat.

  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Protokoll im eingesetzten Informationssystem, Kennzeichen in der Benutzerverwaltung oder Verwaltung in einem extra Tool
  2. Dokumentation der Vorgangsbearbeitung im eingesetzten Informationssystem oder Zusatzdokumentation außerhalb des eingesetzten Informationssystems
  3. Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem

- **Fall 10:** Stichprobenartige Kontrolle Zugriffe auf verlegte Patienten

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche Personen nach einer Verlegung auf Daten eines Patienten zugriffen.

  Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Personen der verlegenden Station griffen wann auf Daten verlegter Patienten nach ihrer Verlegung zu?
  2. Welche Personen der aufnehmenden Station griffen wann, auf Daten von Patienten zu, die zu ihnen verlegt werden sollen, aber noch nicht Patienten ihrer Station sind.
  3. Aus welchen Gründen griffen diese Personen auf die Patientendaten zu?
  4. Wann wurde die Verlegung technisch hinterlegt?

  Spezifikation zur Abbildung der Use Cases:

  Dieser Fall verfolgt eine mögliche Form des missbräuchlichen Datenzugriffs. Nicht für alle Personen ändert sich die Zuständigkeit mit einer Verlegung auf eine andere Station, Beispiel den Verwaltungsmitarbeitern sind die Patienten über Namensräume zugeordnet oder der Patient wird wegen einer komplexen Medikation von einer zentralen Beratung betreut.

  Die Verlegung wird typischerweise in der Patientenverwaltung / Aufenthaltsdokumentation dokumentiert. Technisch kann man den Zeitpunkt der organisatorischen Verlegung und den

Zeitpunkt der Dokumentation im Informationssystem unterscheiden. In den meisten Häusern kann nicht erwartet werden, dass der dokumentierte Zeitpunkt Minuten genau dem tatsächlichen Zeitpunkt entspricht, der Tag der Verlegung sollte jedoch verlässlich dokumentiert sein.
Bei Ärzten und Pflegekräften (deren Zuständigkeit durch die Verlegung wechseln könnte) wird innerhalb des Zugriffs im Rahmen der Behandlung selten der Zweck des Zugriffs dokumentiert, weshalb der Grund des Zugriffs meist erfragt werden muss.
Die Analyse des technischen Dokumentationszeitpunktes ist nur wichtig, wenn die Dokumentation der Verlegung auch die Zugriffsrechte steuert.
Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

1. Protokoll im eingesetzten Informationssystem
2. Protokoll im eingesetzten Informationssystem
3. Entweder aus dem Berechtigungskonzept sowie der dessen Umsetzung im Informationssystem, der Dokumentation des Zugriffs im eingesetzten Informationssystem oder durch Befragen der Person
4. Zusatzinformation im eingesetzten Informationssystem

- **Fall 11:** Stichprobenartige Kontrolle, welche nicht ihren Rollen entsprechende Rechte Beschäftigte haben

  Beschreibung Use Case:

  Im Rahmen einer stichprobenartigen Auswertung prüft der Datenschutzbeauftragte, welche Rechte Beschäftigte haben, die nicht den im Berechtigungskonzept festgelegten Rechten entsprechen. Für die Beantwortung der Fragestellung sind folgende Informationen erforderlich, welche die Protokolle enthalten müssen oder die auf andere Weise bereitgestellt werden müssen:

  1. Welche Beschäftigte haben andere Rechte, als sie entsprechend Berechtigungskonzept haben sollten?
  2. Aus welchen Gründen haben diese Personen andere Rechte, als sie entsprechend Berechtigungskonzept haben sollten?
  3. Seit wann haben diese Personen andere Rechte, als sie entsprechend Berechtigungskonzept haben sollten?
  4. Werden diese anderen Rechte entsprechend in Anspruch genommen und sind somit als gerechtfertigt anzusehen?

  Spezifikation zur Abbildung der Use Cases:

  Idealerweise hat die Einrichtung sowohl ein Berechtigungskonzept, in welchem die Rollen, entsprechende Rechte, etc. als Vorgabe beschrieben sind, und ein Vorgangsbearbeitungssystem über das konkrete Rechte beantragt und deren Gewährung dokumentiert wird.
  Da typischerweise Rechte in Rollen, Gruppen oder Profilen zusammengefasst werden, werden zusätzliche Werkzeuge benötigt, die auswerten, welche elementaren Rechte der Benutzer hat bzw. haben sollte.
  Die benötigten Informationen finden sich wie folgt (Reihenfolge wie im Use Case):

  1. Abgleich Berechtigungskonzept und dessen Umsetzung im eingesetzten Informationssystem
  2. Protokoll im eingesetzten Informationssystem, zusätzliche Informationen aus der dokumentierten Beantragung der Rechte
  3. Protokoll im eingesetzten Informationssystem
  4. Protokoll-im Informationssystem

5 Best Practices

5.1 Organisatorische Rahmenbedingungen schaffen

1. Ein Datenschutzbeauftragter benötigt für eine Prüfung immer Unterstützung durch die IT bzw. eine fachverantwortliche Person, d. h. hier sollten entsprechende Regelungen festgehalten werden.
2. Ebenso sollte die Frage bzgl. Einbeziehung des Betriebsrates geklärt werden
3. Datenschutzprojektgruppe gestalten
   - Interdisziplinäre Datenschutzprojektgruppe ins Leben rufen, welche aus:
     - IT-Leiter,
     - KIS-Verantwortlicher,
     - Kaufmännische Leitung,
     - Personalleitung,
     - Ärztlicher Direktor,
     - Betriebsrat,
     - Pflegedirektion,
     - Datenschutzbeauftragter,
     - Sekretariatspersonal zur Protokollführung
     - entsprechend Fragestellung ggf. weitere Fachpersonen

     besteht und die sich ein bis viermal im Jahr trifft, um Datenschutzthemen abzustimmen.
   - Das Gremium gibt insbesondere auch das jeweilige Berechtigungs-, Protokollierungs- und Löschkonzept frei und setzt diese für die Einrichtung/Organisation in Kraft. Dadurch werden die Rahmenbedingungen für die Protokollauswertungen wie z. B. zeitlicher Abstand oder wer unterstützt den Datenschutzbeauftragten festgelegt.
4. Festlegung von Standardvorgehensweisen („Standard Operating Procedures“, SOP) für eine Protokollauswertung,
   - d. h. wie ist das Vorgehen bei anlassunabhängigen und bei anlassabhängigen Auswertungen,

   aber z. B. auch SOP hinsichtlich
   - Rechtebeantragung von Nutzern inkl. der Berechtigung für die Nutzung von Sonderberechtigungen wie Notfallzugriffen,
   - Zugang von externen Personen wie beispielsweise MDK oder externes Abrechnungspersonal,
   - inhaltlicher Art, d. h. was in den Protokollen von welchen Informationssystemen zu finden ist,
   - usw.

5.2 Technische Rahmenbedingungen schaffen

1. Kontrollsystem (z. B. SolarWinds Access Rights Manager, ehemals 8Man)
2. Erfassen von Begründungen
   - Notfallzugriff mit Begründung
   - Technisch bieten die Zugriffe, nachdem der Patient das Krankenhaus verlassen hat und die Zugriffe von fach-/organisationsfremden Personen erfolgen, eine Herausforderung. Hier wäre es sinnvoll, wie bei einem Notfallzugriff zu Beginn des Zugriffs die Eingabe einer Begründung zu fordern, zu protokollieren und auszuwerten.
3. Einfacher Benutzerwechsel / virtuelle Endgeräte
   - In Arbeitssituationen, in denen sich mehrere Mitarbeiter räumlich eine begrenzte Anzahl von Endgeräten teilen z. B. Station im Krankenhaus, kann man durch virtuelle Arbeitsplätze jedem Mitarbeiter ein virtuelles Endgerät für seine persönliche Anmeldung geben.

6 F.A.Q.

Gerade im Umfeld der niedergelassenen Versorgung kommt es häufig dazu, dass aus Gründen der Arbeitserleichterung Zugriffe nicht einer bestimmten Person zugeordnet werden können. Aber auch im niedergelassenen Umfeld gelten die Erfordernisse der DS-GVO, auch bzgl. der Gewährleistung der Auskunftspflicht gegenüber Patienten oder der Rechenschaftspflicht gegenüber Datenschutz-Aufsichtsbehörden oder anderen ermittelnden Behörden. Im Folgenden werden einige Fälle dargestellt, die möglicherweise eine Einschränkung der Gewährleistung der gesetzlich verankerten Pflichten durch die jeweiligen Verantwortlichen bedeuten können.

6.1 Sammelanmeldung

Beschreibung:

- Alle Mitarbeiter der Anmeldename „Praxis“, Kennwort „Praxis“
- Dies gilt an allen Arbeitsstationen (meist inkl. Server)
- Problematik: Es ist nicht nachvollziehbar, wer welche Eingaben tätigt oder Änderungen vornimmt, da alle Mitarbeiter dasselbe Passwort verwenden
- Lösung: jeder Mitarbeiter erhält eigene Zugangsdaten

Problembeschreibung:

- Eine Protokollierung ist in dieser Konstellation grundsätzlich möglich.
- Jedoch kann mit dieser Protokollierung nur der Tatbestand einer Verarbeitung festgestellt werden, nicht jedoch, welche Person eine Verarbeitung vornahm.

Bewertung:

- Ohne eigene Zugangsdaten pro Benutzer kann nicht nachvollzogen werden, welcher Benutzer Zugriff hatte. Jegliche Verarbeitung kann somit nicht einem Benutzer zugeordnet werden und das ist als sehr kritisch zu bewerten.

6.2 Gleicher Benutzer in verschiedenen Bereichen/Abteilungen

Beschreibung:

- Mitarbeiter arbeitet im selben Haus bspw. auf Station in der Klinik und teilweise im angebundenen MVZ
- Somit hat der Mitarbeiter in der Klinik auf Station Zugriff auf die entsprechenden Daten und gleichzeitig mit derselben Anmeldung Zugriff auf die MVZ-Daten und andersherum, obwohl der Mitarbeiter nur jeweils für den entsprechenden Bereich Zugriff haben sollte
- Lösung: Der Mitarbeiter muss zwei Benutzer für die verschiedenen Tätigkeiten mit jeweiligen Berechtigungen erhalten. Alternativ kann über Rollen und Rechte die Freigabe des Zugriffs auf die jeweiligen Daten im System (Klinik, MVZ) mit den Einstellungen auf den Clients verbunden werden, d. h. das System erkennt, wann der Beschäftigte an einem Klinikrechner angemeldet ist. Somit erfolgt die Freigabe des Zugriffs ausschließlich auf die Klinikdaten und andersherum

Problembeschreibung:

- Eine Protokollierung ist in dieser Konstellation möglich.
- Jedoch kann mit dieser Protokollierung nur der Tatbestand einer Verarbeitung festgestellt werden, nicht jedoch, welche Person eine Verarbeitung vornahm.

Bewertung:

- In dieser Konstellation kann einer betroffenen Person wie einem Patienten nicht mitgeteilt werden, wer auf deren personenbezogene Daten zugegriffen hat, sondern nur ob ein

berechtigter oder unberechtigter Zugriff erfolgte. Somit entspricht diese Konstellation nicht den gesetzlichen Vorgaben hinsichtlich der Auskunftserteilung gegenüber einer betroffenen Person. Dies ist als kritisch zu bewerten.

6.3 Keine personifizierten Anmeldungen

Beschreibung:

- Benutzer werden üblicherweise nach Räumen oder dem Client vergeben, bedeutet:
  - Benutzer: Anmeldung, Kennwort: Anmeldung
  - Benutzer: Labor; Kennwort: Labor
  - Benutzer: Arbeitsplatz 1, Kennwort: Arbeitsplatz 1
- Somit ist zwar nachvollziehbar, wo die Eingabe gemacht wurde, aber nicht welche Person diese getätigt hat
- Lösung: personifizierte Anmeldung pro Mitarbeiter

Problembeschreibung:

- Eine Protokollierung ist in dieser Konstellation möglich.
- Jedoch kann mit dieser Protokollierung nur der Tatbestand einer Verarbeitung festgestellt werden, nicht jedoch, welche Person eine Verarbeitung vornahm.

Bewertung:

- Ohne eigene Zugangsdaten pro Benutzer kann nicht nachvollzogen werden, welcher Benutzer tatsächlich Zugriff hatte. Jegliche Verarbeitung kann somit nicht eindeutig einem Benutzer zugeordnet werden und um Beispiel hat der Benutzer ggf. auch mehr Rechte als überhaupt benötigt. Das ist als sehr kritisch zu bewerten.

6.4 Arztanmeldung

Beschreibung:

- Alle Mitarbeiter in der Praxis melden sich über den abrechnenden Arzt an, bspw. Benutzer: Müller, Kennwort: 1234
- Somit ist nicht nachvollziehbar, welche Eingaben tatsächlich vom behandelnden Arzt getätigt wurden. Noch gravierender ist die Tatsache, dass mit erweiterter Rechtestruktur bei Ärzten Zugriffe auf besonders sensible Daten bestehen können.
- Lösung: Keine Sammelanmeldung über den Arzt-Benutzer

Problembeschreibung:

- Eine Protokollierung ist in dieser Konstellation möglich.
- Jedoch kann mit dieser Protokollierung nur der Tatbestand einer Verarbeitung festgestellt werden, nicht jedoch, welche Person eine Verarbeitung vornahm.

Bewertung:

- Ohne eigene Zugangsdaten pro Benutzer kann nicht nachvollzogen werden, welcher Benutzer tatsächlich Zugriff hatte. Jegliche Verarbeitung kann somit nicht eindeutig einem Benutzer zugeordnet werden und um Beispiel hat der Benutzer ggf. auch mehr Rechte als überhaupt benötigt. Das ist als sehr kritisch zu bewerten.

6.5 Kleine Praxen

Beschreibung:

- In einer Praxis mit nur einem Arzt und ggf. einer Arzthelferin gelten ebenfalls die datenschutzrechtlichen Vorgaben, d. h. auch in diesen Praxen muss dargestellt werden können, wer wann aus welchen Gründen auf welche Daten von welchem Patienten zugegriffen hat. Wenn nur ein Arzt sowie ein Arzthelfer in der Praxis arbeiten, so kann i. d. R.

von einer legitimen Verarbeitung ausgegangen werden, wenn die Patientendaten im Behandlungskontext z. B. bei einem Termin eines Patienten verarbeitet werden. Ein Missbrauch der Daten bzw. eine „Verletzung des Schutzes personenbezogener Daten“ kann aber auch in kleinen Praxen grundsätzlich nicht ausgeschlossen werden, insbesondere unter Berücksichtigung der Tatsache, dass nach Art. 4 Ziff. 12 DS-GVO auch unbeabsichtigte Offenlegungen von bzw. der unbefugte Zugang zu personenbezogenen Daten zu einer Verletzung des Schutzes personenbezogener Daten bedeutet.

Bewertung:

- Ein kleiner Teil der Ausführungen in der Praxishilfe bezieht sich auf die Verpflichtung des Datenschutzbeauftragten entsprechend Art. 39 DS-GVO eine Überwachung der Einhaltung der Datenschutzregelungen bei Verarbeitungen durchführen.
- In einer kleinen Praxis entfällt ggf. die Verpflichtung, einen Datenschutzbeauftragten zu bestellen. Nicht hingegen entfällt die Pflicht für den Verantwortlichen, d. h. den oder die Inhaber der Praxis, die Datenschutzrechtlichen Pflichten zu erfüllen.
- Insbesondere besteht auch ohne benannten Datenschutzbeauftragten für jeden Inhaber einer Arztpraxis die rechtliche Pflicht unabhängig von der Größe der Praxis:
    a) Entsprechend Art. 25 DS-GVO sind die Prozesse der Verarbeitung der personenbezogenen Daten von Beschäftigten oder Patienten so zu gestalten, dass sowohl eine absichtliche als auch eine unbeabsichtigte rechtswidrige Verarbeitung dieser Daten, d. h. jeder Missbrauch, wirksam verhindert wird.
    b) Die Maßnahmen müssen ebenfalls eine wirksame Methode zur Erkennung von „Verletzung des Schutzes personenbezogener Daten“ i. S. v. Art. 4 Ziff. 12 DS-GVO beinhalten.
    c) Gemäß Art. 32 Abs. 1 lit. d DS-GVO sind alle getroffenen Maßnahmen regelmäßig auf ihre Wirksamkeit zu überprüfen, insbesondere auch in Bezug auf „unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten“.
    d) Die entsprechenden Maßnahmen sowie die Überprüfung der Maßnahmen zu dokumentieren. Die Dokumentation dient insbesondere auch als Nachweis i. S. v. Art. 5 Abs. 2 DS-GVO.

    Kann ein Praxisinhaber dies nicht gewährleisten, so wird aufgrund des der Verarbeitung der personenbezogenen Daten innewohnenden hohen Risikos die Benennung eines Datenschutzbeauftragten aufgrund der in § 2 Abs. 2 Nr. 4 BDSG enthaltenen Anforderung vermutlich unabhängig von der Praxisgröße und der Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigen Personen erforderlich sein.
- Weiterhin besteht natürlich die Pflicht der oder des Praxisinhaber, betroffenen Personen eine Auskunft entsprechend den Vorgaben nach Art. 15 DS-GVO zu erteilen. Hierzu gehört insbesondere die Auskunft über
    - die Verarbeitungszwecke wie beispielsweise ein Export von Patientendaten (Art. 15 Abs. 1 lit- a DS-GVO) oder auch
    - die Empfänger von Patientendaten wie beispielsweise Mit- oder Nachbehandelnde, aber auch MDK oder andere gesetzlich vorgeschriebene Akteure (Art. 15 Abs. 1 lit. c DS-GVO).
- Die Frage, wer wann aus welchen Gründen auf die patientenbezogenen Daten zugegriffen hat, kann grundsätzlich mit oder ohne technische Hilfsmittel dargestellt werden. Es besteht immer die Möglichkeit, parallel zum IT-System eine eigene Dokumentation zu führen, mittels derer entsprechende datenschutzrechtlich zu erbringenden Nachweise (Art. 5 Abs. 2 DS-GVO) möglich sind.

7 Abkürzungen

Abs.	Absatz
Art.	Artikel
Artt.	Artikel (Mehrzahl)
BCM	Business Continuity Management
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
bvitg	Bundesverband Gesundheits-IT e.V.
DS-GVO	Datenschutz-Grundverordnung
EGMR	Europäischer Gerichtshof für Menschenrechte (European Court of Human Rights, ECHR)
EHR	Electronic Health Record (dt. ePA)
ePA	Elektronischen Patientenakte
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
HR	Human Resources
ITIL	Information Technology Infrastructure Library
Kap.	Kapitel
KIS	Krankenhausinformationssystem
lit.	littera (lat. „Buchstabe“)
MDK	Medizinischer Dienst der Krankenversicherung
MVZ	Medizinisches Versorgungszentrum / medizinische Versorgungszentren
Nr.	Nummer
PACS	Picture Archiving and Communication System
PVS	Praxisverwaltungssystem
OH	Orientierungshilfe
SGB	Sozialgesetzbuch
SOP	Standard Operating Procedure
Rn.	Randnummer
RStV	Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag)
SOP	Standard Operating Procedure, auf Deutsch etwa Standardvorgehensweise oder standardisiertes Vorgehen
TKG	Telekommunikationsgesetz
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz -)
VIP	„Very Important Person“, also „sehr wichtige Person“; im Kontext des Krankenhauses Personen des öffentlichen Lebens, aber auch u. U. Beschäftigte des Krankenhauses selbst, die Patienten im Krankenhaus, in dem sie arbeiten, sind und deren Daten entsprechend geschützt werden müssen
Ziff.	Ziffer