VINZENZ VON PAUL KLINIKEN gGMBH

MARIENHOSPITAL STUTTGART

Umsetzungshinweise der DKG zur OH KIS

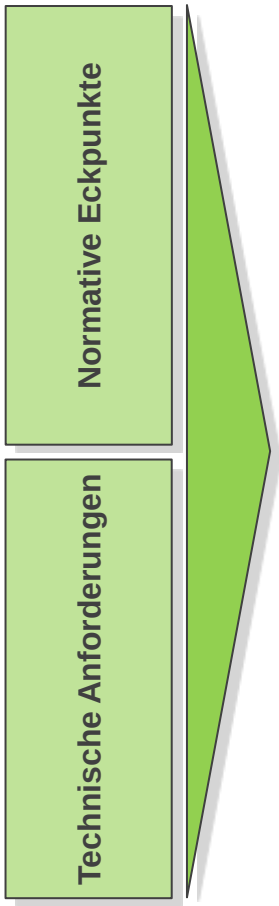
Fachtagung von BWKG und LfD zur Orientierungshilfe Krankenhausinformationssysteme der Datenschutzbeauftragten von Bund und Ländern am 19. Juni 2013

Jürgen Flemming, IT-Leiter
Vinzenz von Paul Kliniken gGmbH, Stuttgart

AGENDA

- **Überblick**
- **Rollen- und Berechtigungskonzept**
- **Protokollkonzept**
- **Lösch-, Sperr- und Auslagerungskonzept**
- **Sicherheitskonzept**
- **Fazit**

Sowohl die Eckpunkte als auch die technischen Anforderungen der OH KIS können durch wenige Kern-Konzepte abgebildet werden



Rollen- und Berechtigungskonzept

- Differenzierte Ausgestaltung bildet den Tagesbetrieb ab
- Protokollierung entsprechend reduziert

Protokoll-Konzept

- Detaillierte Protokollierung, wo über Notfall- oder Sonderzugriffe gearbeitet wird
- Differenziertes Konzept stellt Datensparsamkeit sicher

Berichts- und Reporting Konzept

- Regelmäßige Auswertung der Protokolle unter datenschutzrechtlichen Gesichtspunkten
- Stark eingeschränkter Nutzerkreis

Lösch-, Sperr- und Auslagerungskonzept mit Fallabschluss-Konzept

- Gemäß dem individuellen Fallabschluss-Konzept erfolgt Sperre, Auslagerung ins elektronische Archiv oder Löschung der Daten

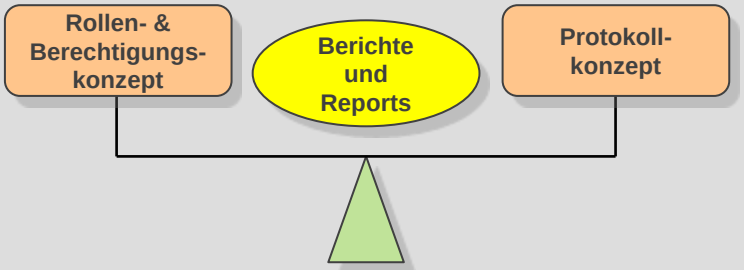
Sicherheitskonzept (Allgemein, Verschlüsselung, MA / VIP, IT-Architektur)

- Ausformulierte IT-Architektur sorgt für Transparenz über Sicherheitsmaßnahmen
- Physischer Zugangsschutz zum RZ vermeidet überflüssige Verschlüsselung
- Exportierte Daten grundsätzlich entweder anonymisiert / pseudonymisiert oder verschlüsselt
- Schutz von Mitarbeitern oder VIP über das Rollen- und Berechtigungskonzept

Vom Krankenhaus zu erstellen und mit Datenschutz abzustimmen

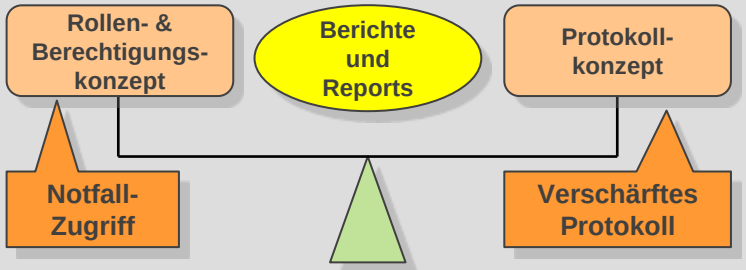
Die Verbindung der Konzepte sorgt für den leistungsfähigen Datenschutz im Krankenhaus – den Kern bilden aber RBK und Protokoll-Konzept

Gleichgewicht zwischen Rollen- und Berechtigungskonzept auf der einen Seite und dem Protokoll-Konzept auf der anderen Seite



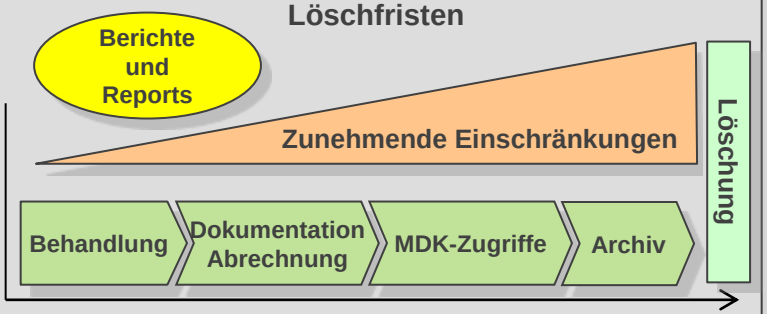
SOLL-Prozesse im Regel-Betrieb

Gleichgewicht zwischen Rollen- und Berechtigungskonzept auf der einen Seite und dem Protokoll-Konzept auf der anderen Seite



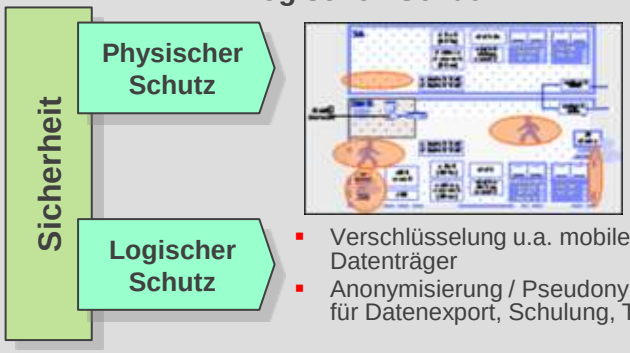
SOLL-Prozesse im Not-Betrieb

Fallabschluss-Konzept als Grundlage für die Definition der Sperr-, Auslagerungs- und Löschfristen



Schematische Beispiel-Darstellung

Sicherheitskonzept sorgt für den physischen und logischen Schutz



- Verschlüsselung u.a. mobiler Datenträger
- Anonymisierung / Pseudonymisierung für Datenexport, Schulung, Test

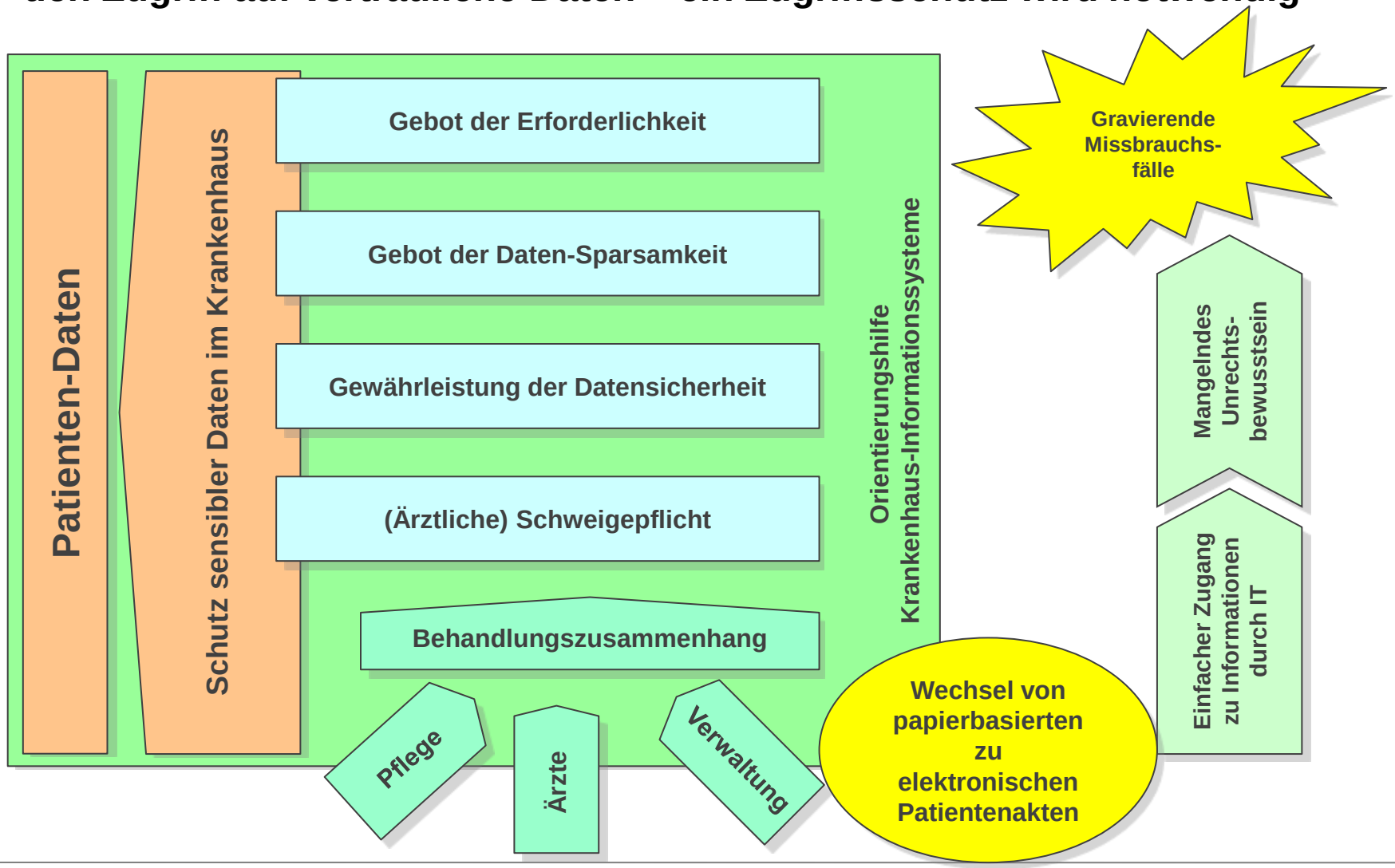
Die Umsetzungshinweise der DKG informieren über die Anforderungen des Datenschutzes und bieten Arbeitshilfen zu deren Umsetzung

- Die Umsetzungshinweise der DKG wurden von einer Arbeitsgruppe des Fachausschusses Daten- und Informationskommunikation zwischen 2011 und 2013 erarbeitet
- Sie sollen die Schwerpunkte der OH KIS für das Krankenhaus praxisgerecht aufbereiten und praktische Anleitung zur Umsetzung geben
- Der Aufbau folgt der Konzeptstruktur und nimmt keinen Bezug auf konkrete Teilziffern der OH KIS
- Im Anhang sind Mustervorlagen als konkrete Arbeitshilfen zu finden
- Der wesentliche Anspruch dieser Umsetzungshinweise ist die für Krankenhausmitarbeiter verständliche Aufbereitung der Anforderungen des Datenschutzes

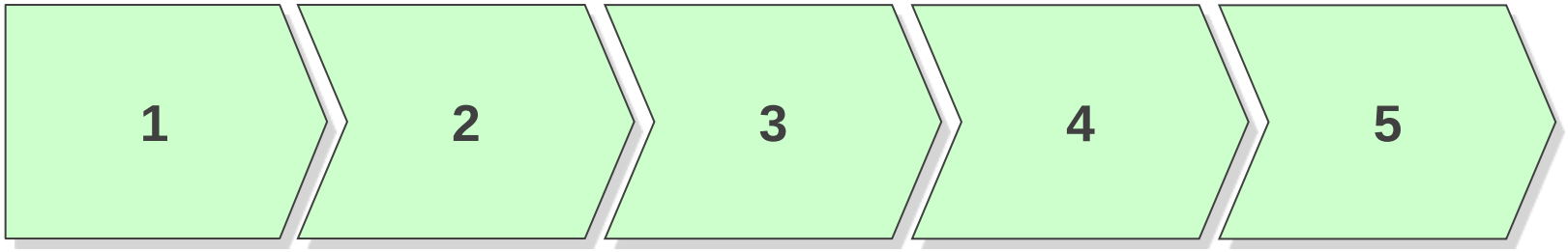
AGENDA

- Überblick
- **Rollen- und Berechtigungskonzept**
- Protokollkonzept
- Lösch-, Sperr- und Auslagerungskonzept
- Sicherheitskonzept
- Fazit

Der Technologiewechsel zur elektronischen Patientenakte vereinfacht den Zugriff auf vertrauliche Daten – ein Zugriffsschutz wird notwendig

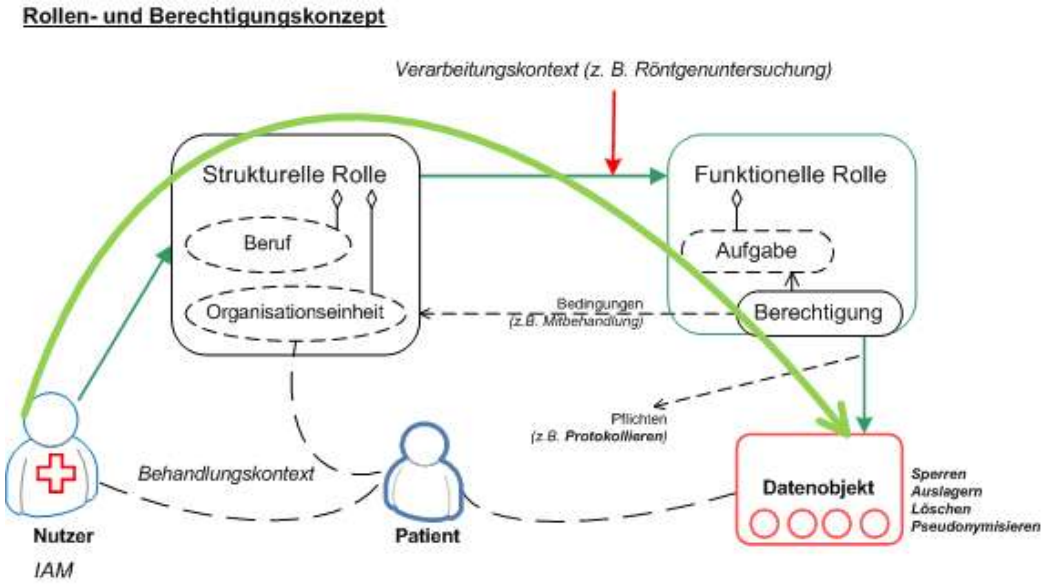


Die Rollen und zugehörigen Zugriffsrechte können in 5 Schritten relativ einfach erarbeitet werden



1	2	3	4	5
Vollständige Auflistung aller **Organisations-einheiten**, in denen Mitarbeiter in Wahrnehmung ihrer Arbeits-aufgaben Patientendaten nutzen müssen	Vollständige Zuordnung aller **Mitarbeiter** zu den Organisations-einheiten	Vollständige Auflistung aller **Aufgaben** der Mitarbeiter in der Organisationsein heit unter Berücksichtigung ihrer beruflichen Qualifikation und Stellung innerhalb der Aufbau- und Ablauf-organisation	Vollständige Auflistung und Kategorisierung aller für die Aufgaben-wahrnehmung benötigten **Patientendaten** („Datenobjekte“) mit ihrer konkreten Präsentations-form (z. B. Bild-schirmmaske, Berichts-dokument, Einzelmerkmal)	Festlegung der erforderlichen **Zugriffs-methoden** (z. B. Erstellen, Schreiben, Ändern, Lesen), Entscheidung über Gruppenzugriffe

Die funktionale und die strukturelle Rolle des Anwenders definieren die notwendigen Zugriffsrechte

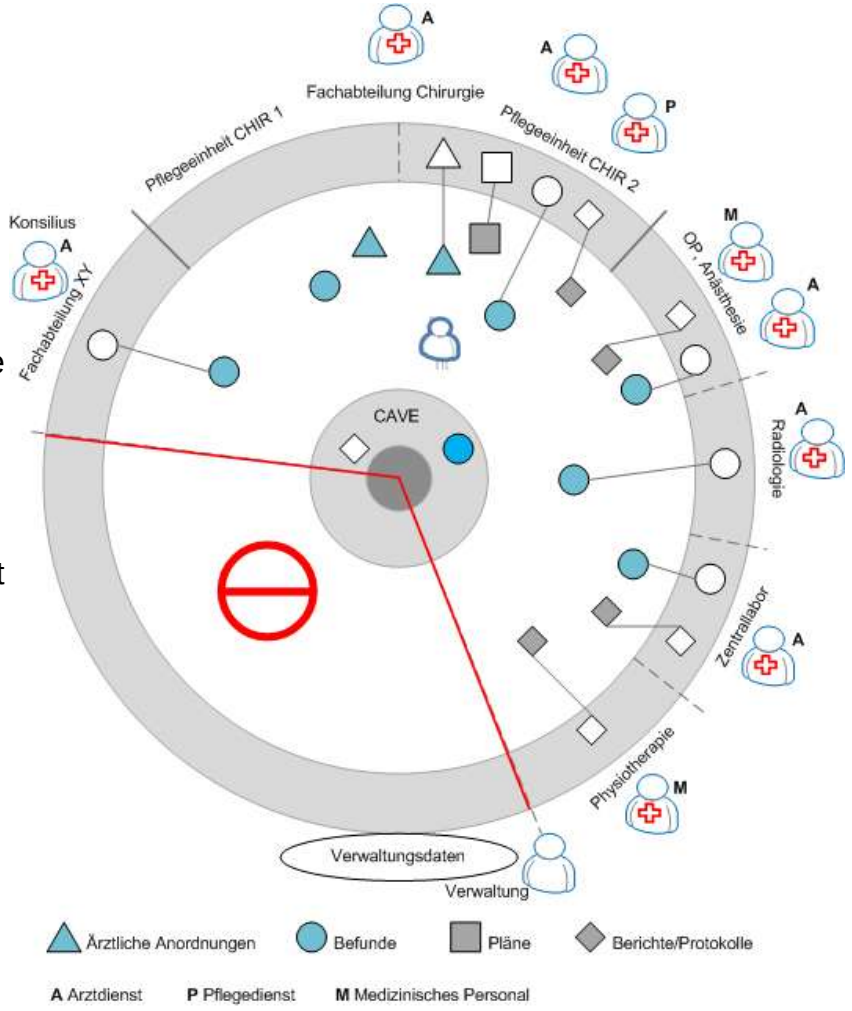


- **Strukturelle Rolle:** wird abgeleitet aus der Zugehörigkeit zu einer bestimmten Organisationseinheit und dem ausgeübten Beruf
- **Funktionelle Rollen** definieren die Beteiligung an der Behandlung eines Patienten und damit das Recht, Einblick in die Patientendaten im benötigten Umfang zu nehmen oder die Patientendaten durch eigene Einträge fortzuschreiben
- **Organisatorische Maßnahmen** können dazu beitragen, das Rollen- und Berechtigungskonzept durchzusetzen, z. B. durch die zeitnahe Datenschutzauswertung von (geschützten) Protokollen in kontrollierter, datenschutzkonformer Form

***Quelle**: Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme, Stand 06.06.2013*

Strukturierung der Patientendaten in Stamm-, CAVE- und abteilungs-spezifische medizinische, pflegerische oder administrative Daten

- Im Mittelpunkt befinden sich **Patienten-stammdaten**, die zur Feststellung der Identität des Patienten allen Mitarbeitern zur Verfügung stehen müssen, die patientenbezogen Aufgaben in Bezug auf den Krankenhausaufenthalt wahrnehmen
- Die Patientenstammdaten sind umgeben von wichtigen medizinischen Informationen, z. B. über bekannte Allergien oder Arzneimittelunverträglichkeiten des Patienten. Diese Daten, müssen zur Vermeidung von Zwischenfällen allen medizinischen Mitarbeitern zur Verfügung stehen (**CAVE-Daten**)
- Darum herum gruppieren sich die **medizinischen Informationen der aktuellen Behandlung**, ggf. mit Vorbehandlungsdaten wie z. B. Arztbriefe, Berichte, Befunde, Pflegeinformationen



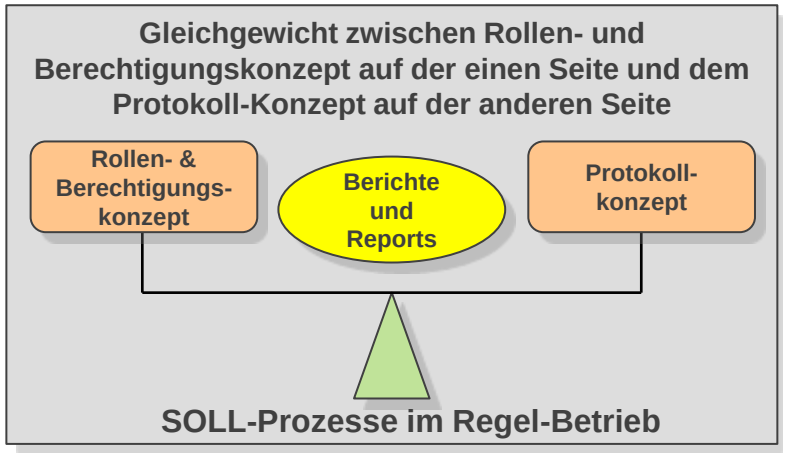
***Quelle**: Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme, Stand 06.06.2013*

AGENDA

- Überblick
- Rollen- und Berechtigungskonzept
- **Protokollkonzept**
- Lösch-, Sperr- und Auslagerungskonzept
- Sicherheitskonzept
- Fazit

Der Detailgrad der Protokollierung hängt stark von der Differenzierung des Rollen- und Berechtigungskonzepts ab

- Die Protokollierung muss nachvollziehbar dokumentieren, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat
- Die Protokollierung korrespondiert mit den bestehenden Zugriffsregelungen. Bei hinreichend eng ausgestaltetem Zugriffsschutz können die Anlässe der Protokollierung in Verbindung mit dem Rollen- und Berechtigungskonzept reduziert werden
- Die Mitarbeiter müssen über die Anlässe ihrer Protokollierung, ihre Einsichtsmöglichkeit in die Protokolle und die datenschutzkonforme Verarbeitung, Nutzung und Löschung der Protokolldaten unterrichtet werden
- Im Regelfall sollen Protokolldaten für 12 Monate aufbewahrt werden. Mit dem Wegfall der Erforderlichkeit für die Aufgabenerfüllung sind die gespeicherten Protokolldaten zu löschen



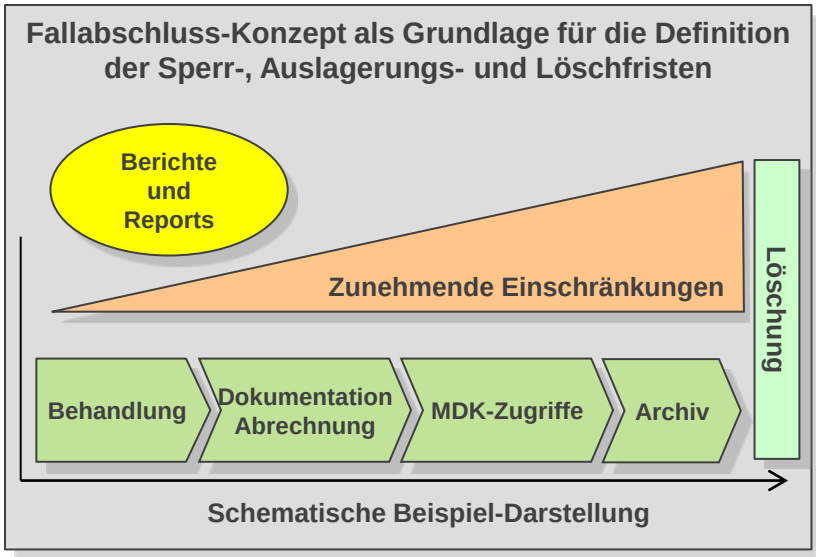
Die Auswertung der Protokollierung muss dem **engen Kreis der dafür Berechtigten** ermöglichen festzustellen, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat oder unberechtigt nutzen wollte

AGENDA

- Überblick
- Rollen- und Berechtigungskonzept
- Protokollkonzept
- **Lösch-, Sperr- und Auslagerungskonzept**
- Sicherheitskonzept
- Fazit

Sperrung, Auslagerung oder Löschung von Patientendaten müssen sich an einem klaren Fristenkonzept orientieren

- Der Zugriff auf Patientendaten soll mit Eintritt definierter Ereignisse, die den Abschluss der Behandlung kennzeichnen, durch das **Sperren** (oder das Auslagern) der Daten eingeschränkt werden
- Für die unterschiedlichen Berufsgruppen eines Krankenhauses als auch Patientengruppen sind jeweils verschiedene **Ereignisse und Fristen** zu berücksichtigen, mit denen der Zugriff auf Daten eines Behandlungsfalles nicht mehr notwendig und somit zu begrenzen ist
- Das Krankenhaus muss in sein **Sperrkonzept** eine eindeutige Regelung aufnehmen, welche der möglichen Ereignisse für welche Rollen eine Zugriffsbegrenzung (Sperrung) auslösen müssen
- Die Fristen sollten sich an den **geschäftsüblichen Arbeitsabläufen** orientieren, d. h. die betroffenen Mitarbeiter sollen in der üblichen Durchführung ihrer Aufgaben nicht behindert werden



Als mögliche zugriffsbegrenzende Ereignisse, die den Abschluss eines Behandlungsfalls bestimmen können, kommen in Betracht (Auszug):

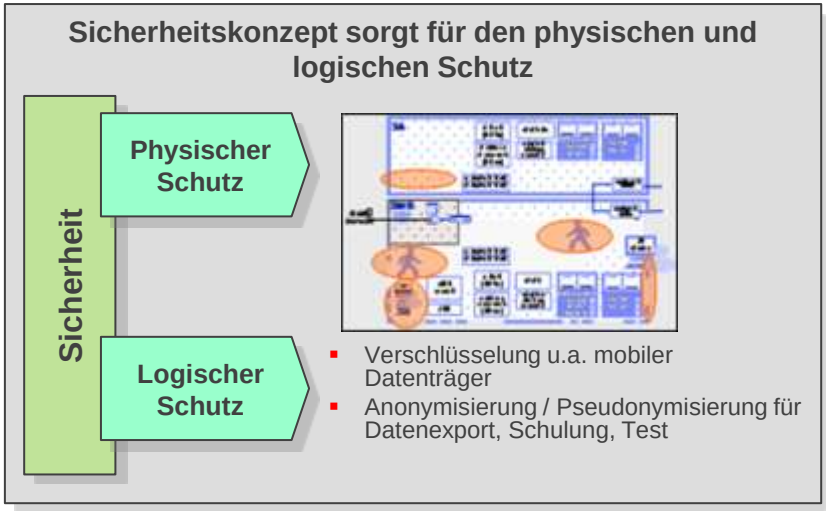
- Abschluss einer Beauftragung mit Zugriffserfordernis auf die Patientendaten,
- Interne Verlegung des Patienten in eine andere Fachabteilung,
- Entlassung des Patienten,
- Übermittlung der Schlussrechnung nach Entlassung,
- Fristablauf für Nachprüfungen zum Behandlungsfall durch den MDK (= 6 Wochen nach Rechnungszustellung),
- ….

AGENDA

- Überblick
- Rollen- und Berechtigungskonzept
- Protokollkonzept
- Lösch-, Sperr- und Auslagerungskonzept
- **Sicherheitskonzept**
- Fazit

Maßnahmen der IT-Sicherheit, sichere Prozesse und anonymisierte Daten tragen zum Schutz der Daten vor unberechtigten Zugriffen bei

- Patientendaten müssen vor unberechtigten Zugriffen geschützt werden. Dies erfolgt entweder durch die Verschlüsselung der Daten oder durch einen physischen und logischen Zugangsschutz
- Für Mitarbeiter, besonders schutzbedürftige Personen oder VIP‘s sollte entweder ein organisatorisches Konzept oder eine technische Lösung implementiert sein
- Insbesondere Wartungszugänge externer Firmen müssen besonders überwacht und kontrolliert werden
- Daten auf mobilen Datenträgern sollten grundsätzlich sicher verschlüsselt werden, da sie nicht mehr der Kontrolle des Hauses unterliegen
- Schulungs- und Test-Daten sollten grundsätzlich anonymisiert werden, Daten für die Forschung sollten pseudonymisiert sein



Insbesondere die Rechenzentren müssen auf den physischen und logischen Schutz der Daten hin geprüft werden

AGENDA

- Überblick
- Rollen- und Berechtigungskonzept
- Protokollkonzept
- Lösch-, Sperr- und Auslagerungskonzept
- Sicherheitskonzept
- Fazit

Die Umsetzungshinweise der DKG informieren über die Anforderungen des Datenschutzes und bieten Arbeitshilfen zu deren Umsetzung

- Die OH KIS bündelt bestehende Vorschriften des Datenschutzes
- Der Prozess der Veröffentlichung und der nachfolgenden Diskussion hat insbesondere im Krankenhaus das Bewusstsein für den Datenschutz gefördert – auch wenn die Diskussion nicht immer spannungsfrei erfolgt
- Das Bewusstsein für den Datenschutz muss nun auch in die Köpfe der betroffenen Mitarbeiter transportiert werden
- Die offene und faire Diskussion zwischen den betroffenen Parteien ist auch in Zukunft entscheidend
- Die Umsetzungshinweise helfen dabei, die eigene Position zu bestimmen

Vielen Dank für Ihre Aufmerksamkeit !

Jürgen Flemming
Vinzenz von Paul Kliniken gGmbH
Böheimstraße 37

70199 Stuttgart

Tel.: 0711 – 6489 – 3490
eMail: Juergen.Flemming@vinzenz.de