Hinweise des
Landesbeauftragten für den Datenschutz Baden-Württemberg
zur Erstellung einer

Zugriffs-, Sperr- und Löschkonzeption für Krankenhaus-EDV-Systeme

- Stand: 09. Juli 2008 -

In Baden-Württemberg dürfen Krankenhäuser nach dem Landeskrankenhausgesetz Angaben über ihre Patienten per Computer speichern und nutzen, soweit dies zu deren medizinischer Versorgung sowie zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses notwendig ist. Um sicherzustellen, dass sich die Datenverarbeitung in diesen Grenzen hält, muss das Krankenhaus, beginnend mit der erstmaligen Speicherung von Daten, im Rahmen einer Zugriffs-, Sperr- und Löschkonzeption regeln, welchen Bediensteten es welche Zugriffsrechte auf welche gespeicherte Daten einräumt und wann welche Daten zu sperren bzw. zu löschen sind. Ziel dieses Merkblatts ist, Krankenhäusern eine Hilfestellung bei der Erstellung einer derartigen Konzeption zu geben.

I. Allgemeines

Auch innerhalb des Krankenhauses gilt die ärztliche Schweigepflicht. Daran sowie an dem auch in § 45 Abs. 1 des Landeskrankenhausgesetzes zum Ausdruck kommenden datenschutzrechtlichen Grundsatz der Erforderlichkeit haben sich etwaige Zugriffsrechte auf Patientendaten auszurichten. Dabei ist zu beachten, dass das Krankenhaus datenschutzrechtlich keine Einheit darstellt. Die einzelnen Funktionsbereiche, wie etwa die Verwaltung oder die einzelnen Fachabteilungen, sind jeweils für sich zu sehen. Bei der Ausgestaltung von Zugriffsberechtigungen in einem Krankenhausinformationssystem ist dies zu berücksichtigen.

II. Zugriffskonzeption

Nach dem Datenschutzrecht darf das Krankenhaus jeder seiner funktionalen Einheiten und jedem der in diesen Einheiten Beschäftigten nur die Zugriffsrechte auf Programme und Daten einräumen, die für die Erfüllung der jeweiligen Aufgaben tatsächlich benötigt werden. Im Einzelnen bedeutet dies Folgendes:

– Krankenhausverwaltung
  Die Krankenhausverwaltung darf nur auf die Daten zugreifen können, die sie zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses, insbesondere zur Abrechnung der erbrachten Leistungen, benötigt.

– Innerhalb der behandelnden Abteilung
  Innerhalb der behandelnden Fachabteilung müssen den Ärzten sowie den Pflegekräften die für die Sicherung des Behandlungserfolgs erforderlichen Daten zur Verfügung stehen. Entsprechend der jeweiligen Funktion des ärztlichen und des Pflegepersonals ergeben sich unterschiedliche Zugriffsnotwendigkeiten. Dies erfordert eine Binnendifferenzierung der Zugriffsmöglichkeiten. Beispiele:

  • Ärzte
    Im Regelfall genügt es, wenn ein Arzt lesenden und schreibenden Zugriff auf die Daten der Patienten hat, an deren Behandlung er aktuell mitwirkt. Dies können auch Daten aus früheren Behandlungen sein. Ist ein Patient entlassen, dürfen seine Daten nur so lange zur Verfügung stehen, bis der Entlassungsbericht geschrieben

ist. Der Zugriff auf die Patientendaten darf erst wieder im Zusammenhang mit einer neuen Behandlung eröffnet werden.

- Pflegepersonal
  Für Pflegepersonal genügt in der Regel lesender und - in klar begrenztem Umfang - u. U. auch schreibender Zugriff auf Daten von Patienten der eigenen Station. Der Zugriff ist zu entziehen, sobald der Patient entlassen oder auf eine andere Station verlegt wird.

– Zwischen Abteilungen
  Grundsätzlich darf jede Abteilung nur Zugriff auf die eigenen Daten haben. Wurde ein Patient bereits früher in einer anderen Abteilung des Krankenhauses behandelt und sind die dort vorhandenen Informationen nach ärztlicher Einschätzung für die aktuelle Behandlung erforderlich, darf der Zugriff der behandelnden Abteilung auch auf diese Daten eröffnet werden. Die Initiative hierzu muss von der behandelnden Abteilung ausgehen, die Entscheidung über die Freigabe "ihrer" Daten muss die ersuchte Abteilung treffen. Keinesfalls darf es so sein, dass jede Abteilung technisch in der Lage ist, selbständig auf alle medizinischen Daten einzelner oder aller Fachabteilungen zuzugreifen. Nach Abschluss der Behandlung sind die Zugriffsmöglichkeiten wieder zu sperren.

– Gemeinsame Behandlung
  Wird ein Patient im Verlauf des Krankenhausaufenthalts in eine andere Abteilung verlegt, gestattet die bisher behandelnde der übernehmenden Abteilung den Zugriff auf "ihre" Daten, soweit ein Behandlungszusammenhang besteht und diese Daten aus medizinischer Sicht für die Weiter- oder Mitbehandlung erforderlich sind. Der Zugriff ist nach Abschluss der Behandlung wieder zu sperren. In Fällen, in denen ein Patient typischerweise in mehreren Abteilungen behandelt wird (z. B. Geburtshilfe und Kinderklinik), kann die Klinikumsleitung festlegen, dass die jeweiligen Zugriffsrechte von vornherein bestehen.

– Weitere Einrichtungen
  Patientendaten dürfen an Einrichtungen zur sozialen Betreuung sowie an Einrichtungen, die die pflegerische Versorgung der Patienten übernehmen und an Angehörige sowie sonstige Bezugspersonen nur übermittelt werden, wenn der Patient hierüber vorab informiert wird und dem nicht widersprochen hat.

– Notfallberechtigung
Die Frage der sog. "Notfallberechtigung" ist besonders heikel. Ein Zugriff auf ausnahmslos alle Daten, die im Krankenhausinformationssystem gespeichert sind, dürfte auch im Notfall meist nicht erforderlich sein. Vielmehr müssen dem behandelnden Arzt im Notfall nur die Informationen zur Verfügung stehen, die er braucht, um eine gegenwärtige akute Gefahr für den Patienten abzuwehren (z. B. Blutgruppe, Allergien, Medikamentenunverträglichkeit, usw.). Er wird in der konkreten Notsituation ohnehin faktisch kaum in der Lage sein, alle im System gespeicherten Unterlagen einzusehen und auszuwerten. Insofern sollte ein Notfalldatensatz definiert und im System bereitgestellt werden. Im Notfall kann auf diesen mittels einer besonderen Berechtigung zugegriffen werden. Die Zugriffe sind zu protokollieren und regelmäßig auszuwerten. Hierauf ist vor der Eröffnung des Zugriffs systemtechnisch deutlich hinzuweisen.

III. Sperr- und Löschkonzeption

– Speicherdauer
Nach der Berufsordnung der Landesärztekammer Baden-Württemberg sind Patientendaten für einen Zeitraum von 10 Jahren nach der letzten ärztlichen Behandlung aufzubewahren. In der Praxis orientieren sich viele Krankenhäuser allerdings nicht an dieser 10-Jahres-Frist, sondern an den Fristen des BGB zur Geltendmachung von Schadenersatzansprüchen. Diese liegen bei 30 Jahren. Hinzuweisen ist allerdings darauf, dass keine Rechtsvorschrift existiert, die eine 30-jährige Speicherung von Krankenakten oder elektronisch gespeicherten Patientendaten zulässt oder zwingend vorschreibt. Einen Automatismus, medizinische Unterlagen generell 30 Jahre lang vorzuhalten, darf es jedenfalls nicht geben, da erfahrungsgemäß solche Ersatzansprüche schon wesentlich früher geltend gemacht werden. So ist in folgenden Fällen eine Löschung von Patientendaten auch schon vor Ablauf von 30 Jahren, u.U. auch schon vor Ablauf von 10 Jahren, angezeigt:

- Die gespeicherten Patientendaten sind nur von geringem Nutzen.
- Die Speicherung ist unzulässig (z. B. Erfassung unrichtiger Daten).
- Der Patient verlangt die Löschung und die behandelnden Abteilungen sowie die beteiligten Dritten stimmen zu.

In medizinisch begründeten Fällen (z. B. bei Erkrankungen im Kindesalter oder bei Erbkrankheiten) kann eine Speicherung von Patientendaten über die 30 Jahre hinaus

vertretbar sein. Eine solche längerfristige Speicherung muss aber stets im Einzelfall von den Ärzten entschieden werden.

Unberührt von dem bisher Gesagten bleibt die Möglichkeit, Daten längerfristig zu speichern, falls das Krankenhaus die Daten anonymisiert. Ein Personenbezug darf danach nicht mehr herstellbar sein.

– Sperrung von Daten
  Bei elektronisch gespeicherten Patientendaten ist im Regelfall eine direkte Zugriffsmöglichkeit auf sämtliche Daten über einen Zeitraum von 30 Jahren nicht notwendig. Vielmehr gilt Folgendes:
  - Sind Patienten entlassen und ist der Entlassungsbericht geschrieben, wird der Zugriff auf einige wenige Angaben (z. B. Name, Vorname, Geburtsdatum) beschränkt, die ausreichen, um im Falle einer erneuten Aufnahme den Patienten identifizieren und feststellen zu können, ob noch weitere Daten über ihn gespeichert sind. Die restlichen über diesen Patienten gespeicherten Angaben werden gesperrt. Den zugriffsberechtigten Benutzern wird angezeigt, dass noch weitere Angaben über den Patienten gespeichert sind. Unberührt hiervon bleibt der Notfalldatensatz.
  - Wird ein Patient erneut im Krankenhaus stationär behandelt und sind zu diesem Patienten Daten gesperrt, so können diese zum Zweck der aktuellen Behandlung entsperrt und somit für den Zugriff wieder freigegeben werden.