Abschlussbericht über die Schwerpunktprüfung des BfD EKD in Krankenhäusern

Einleitung

Im September 2023 startete der BfD EKD in die Schwerpunktprüfung im Bereich der **evangelischen Krankenhäuser**. Der BfD EKD versteht unter einer Schwerpunktprüfung eine **anlasslose Prüfung in einem (verfasst-)kirchlichen oder diakonischen Tätigkeitsfeld** mit dem Ziel der kontinuierlichen Verbesserung des Datenschutzes in den geprüften Einrichtungen. Gemäß § 43 Abs. 1 DSG-EKD haben die Aufsichtsbehörden insbesondere die einheitliche **Anwendung und Durchsetzung des kirchlichen Datenschutzrechtes** in ihrem Zuständigkeitsbereich zu überwachen und sicherzustellen. Dazu gehören auch (insbesondere) Prüfungen von kirchlichen und diakonischen Stellen. Auch die **Rechtsprechung des Europäischen Gerichtshofs (EuGH)** macht deutlich, dass die Aufsichtsbehörden ihre Aufgaben erst dann umfassend erfüllen, wenn nicht nur anlassbezogene, sondern auch anlasslose Prüfungen erfolgen. Im Ganzen ist es somit das Ziel der **Schwerpunktprüfungen**, den Datenschutz in den zu prüfenden Einrichtungen zu verbessern sowie die gesetzlichen Aufgaben im Rahmen der Vorgaben des EuGH zu erfüllen.

Geprüft wurden ekd-weit insgesamt **20 evangelische Krankenhäuser**. Die Schwerpunktprüfung wurde mit einem Online-Fragebogen durchgeführt und ergänzt durch die Anforderung von Dokumenten und die Durchführung von Vor-Ort-Terminen.

Alle konkret zitierten Paragrafen aus dem EKD-Datenschutzgesetz beziehen sich auf die im Prüfzeitraum geltende Fassung, soweit nicht ausdrücklich etwas anderes gekennzeichnet ist.

Ablauf der Schwerpunktprüfung

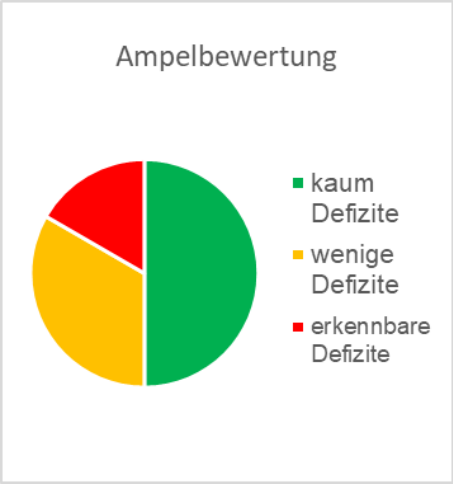
Zur Sicherstellung eines standardisierten Verfahrens und um eine belastbare Datenqualität zu erreichen, wurde ein **Online-Fragebogen** verwendet.

Der Fragebogen wurde von einer internen Arbeitsgruppe erstellt. Zusätzlich wurden ein **Bewertungsmaßstab** für die spätere Auswertung der Antworten und ein **Gesprächsleitfaden** für die Vor-Ort-Prüfungen entwickelt, um eine einheitliche Qualität der Einzelprüfungen zu gewährleisten.

Die Open Source Software **„Limesurvey“** wurde erneut ausgewählt, um den Online-Fragebogen zu realisieren. Auch bei dieser Schwerpunktprüfung erfolgte die Umsetzung mit einem Dienstleister in einem deutschen Rechenzentrum.

Die zu prüfenden Krankenhäuser wurden **innerhalb der Diakonischen Landesverbände zufällig ausgewählt** und postalisch informiert. Alle Krankenhäuser bekamen ihren **individuellen Zugangsschlüssel** zum Fragebogen mit einer Frist von mehreren Wochen, um den Fragebogen online aus-

zufüllen und die erforderlichen Dokumente hochzuladen. Zeitgleich wurden die Diakonischen Landesverbände darüber informiert, welche Krankenhäuser in ihrem Bereich geprüft werden sollen. Auch der Fragebogen wurde zur Kenntnis gegeben.



Die **Rücklaufquote** nach Ablauf der Frist war hoch. Wenige Krankenhäuser mussten an die Abgabe der Antworten erinnert werden.

Am Hauptsitz des BfD EKD wurden zunächst alle Fragebögen mit Hilfe eines **Ampelsystems** summarisch geprüft. Etwa die Hälfte der Einrichtungen wurde im Ampelsystem bei der ersten Prüfung als „grün“ kategorisiert, da auf den ersten Blick keine offensichtlichen Datenschutzmängel erkennbar waren. Bei den „gelben“ und „roten“ Fragebögen wurde vorgeschlagen, Dokumente zur tieferen Prüfung des Datenschutzniveaus in den Einrichtungen anzufordern oder auch eine Vor-Ort-Prüfung durchzuführen. Auch Rückfragen zu den Antworten aus den Fragebögen waren für die abschließende Prüfung teilweise erforderlich.

Zu diesem Zeitpunkt wurde der **Zwischenbericht** zur ersten Schwerpunktprüfung des BfD EKD auf der Internetseite veröffentlicht.

Die abschließende Prüfung und eine **stichprobenhafte Vor-Ort-Prüfung** erfolgten in den jeweils zuständigen Außenstellen und endeten mit entsprechenden **Abschlussschreiben** an das geprüfte Krankenhaus. Diese Schreiben zeigten die Ergebnisse sowie die erkennbar gewordenen Mängel auf und gaben den Krankenhäusern konkret umzusetzende Anforderungen und Empfehlungen an die Hand.

Mit der Erstellung und Veröffentlichung dieses **Abschlussberichts** endet die Schwerpunktprüfung in evangelischen Krankenhäusern des BfD EKD.

Ergebnisse der Schwerpunktprüfung

Der Fragebogen umfasste **65 Fragen**. Neben allgemeinen Angaben wurden Fragen zum rechtlichen und organisatorischen Umfeld sowie zum technischen Umfeld gestellt. Dabei waren überwiegend mehrere Antwortmöglichkeiten vorgegeben und häufig auch Freitextfelder vorgesehen. Ein Schwerpunkt lag auf dem Einsatz des **Krankenhausinformationssystems (KIS)**.

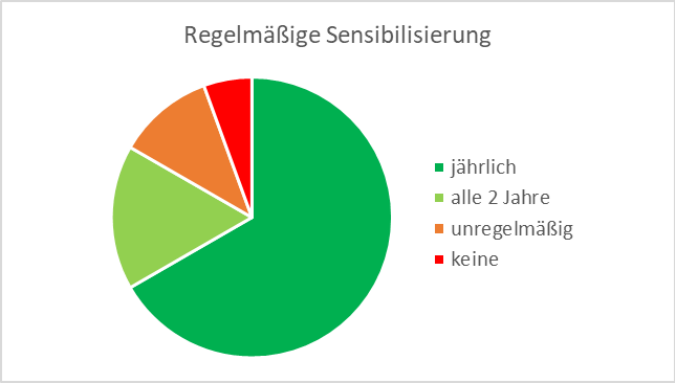
Angaben zur oder zum örtlich Beauftragten für den Datenschutz

Die rechtliche Verpflichtung, eine oder einen **örtlich Beauftragte(n) für den Datenschutz** gemäß § 36 Abs. 1 DSG-EKD zu bestellen, wird erfüllt. Einige Häuser haben externe örtlich Beauftragte für den Datenschutz berufen. Hier muss immer an die Vereinbarung nach § 36 Abs. 5 DSG-EKD gedacht werden. Die gesetzlich **vorgeschriebene Vertretung** ist teilweise noch nicht geregelt. Hier besteht Nachholbedarf in einigen Häusern, der auch klar aufgezeigt wurde. Diese Verpflichtung besteht auch, wenn eine Firma als externer Datenschutzbeauftragter bestellt ist.

Fragen aus dem rechtlichen und organisatorischen Umfeld

Die Auswertung der Fragen aus diesem Bereich ergab, dass erwartungsgemäß bereits ein **hohes Bewusstsein** für die datenschutzrechtlichen Anforderungen vorhanden ist.

Die Verpflichtung auf das **Datengeheimnis** gemäß § 26 DSG-EKD geschieht erfreulicherweise flächendeckend. Auch eine **Sensibilisierung im Umgang mit datenschutzrechtlichen Themen** bei der Einarbeitung gehört überwiegend zum Standard. Eine jährliche Schulung zur Auffrischung und für die Basis eines guten Datenschutzniveaus wurde empfohlen, sofern diese noch nicht etabliert war. In diesem Zusammenhang wurde auch auf Musterfolien und die Lernplattform auf unserer Homepage verwiesen. Positiv ist die Erkenntnis, dass in den meisten Krankenhäusern die **Informationspflichten** gemäß § 17 DSG-EKD aktiv, also nicht erst auf Verlangen, erfüllt werden. Überwiegend geschieht dies durch Beiblätter zu den Verträgen. Auch auf den **Internetseiten** werden diese Informationen teilweise zur Verfügung gestellt. Bezüglich der Informationspflichten wurden die Krankenhäuser in denen bisher keine aktive Erfüllung vorgenommen wurde, auf die **nun bestehende Rechtslage** hingewiesen. Es muss unabhängig von einem Verlangen nun **Zugang zu den Informationspflichten** gewährt werden.



Die Prüfung ergab, dass Patienteninformationen bereits überwiegend im KIS erfasst werden. Das gilt oft auch für die **einzuholenden Einwilligungen**. Damit wird das Risiko minimiert, dass Daten ohne die erforderliche Rechtsgrundlage verarbeitet werden und sichergestellt, dass auch erfolgte **Widerrufe** erfasst und umgesetzt werden können. Dort, wo diese Erklärungen noch in Papier unabhängig von der Patientenakte abgelegt werden, wurde empfohlen, diese Daten im KIS zusammenzuführen. Teilweise war dieser Schritt auch bereits in Planung. Insgesamt macht sich aber hier der bereits **hohe Grad der Digitalisierung positiv** bemerkbar und ist hilfreich bei der Erfüllung der Rechenschaftspflichten.

Der Prozess beim **Umgang mit Datenpannen** sollte in einigen Krankenhäusern noch optimiert werden, insbesondere die **interne Dokumentation** gemäß § 32 Abs. 5 DSG-EKD wird noch nicht überall zufriedenstellend geführt. Diese verpflichtende Dokumentation muss ggf. der Aufsichtsbehörde zur Überprüfung der Einhaltung der Bestimmungen aus § 32 DSG-EKD zur Verfügung gestellt werden. Auch dient diese interne Dokumentation zur Vorbereitung einer **Meldung an die Aufsichtsbehörde**. Ein **klarer Prozess**, der auch die oder den örtlich Beauftragten für den Datenschutz mit einbezieht, ist unerlässlich.

Eine Frage bezog sich auf die Rechtsgrundlagen, auf denen die Krankenhäuser mit **Arztpraxen oder externen medizinischen Dienstleistern kommunizieren**. Hintergrund der Frage war auch die Tatsache, dass mittlerweile in vielen **staatlichen Landeskrankenhausgesetzen** Rechtsgrundlagen existieren, die die Offenlegung von Gesundheitsdaten erlauben, soweit dies im Rahmen der gemeinsamen Behandlung erforderlich ist. Insoweit ist der erforderliche Datenaustausch dann ohne explizite Einwilligung möglich, sondern erfordert nur eine transparente Information. Im Rahmen der Prüfung stellte sich jedoch heraus, dass die Einbindung externer medizinischer Dienstleister weiterhin hauptsächlich auf **Einwilligungsbasis** geschieht. Werden in diesen Fällen Widerrufe geltend gemacht, sind weitere Offenlegungen jedoch grundsätzlich ausgeschlossen.

Eine weitere Frage behandelte die **Einbindung der Krankenhausseelsorge** bzw. die datenschutzrechtliche Umsetzung. Die rechtlichen Grundlagen für die Krankenhausseelsorge basieren auf dem

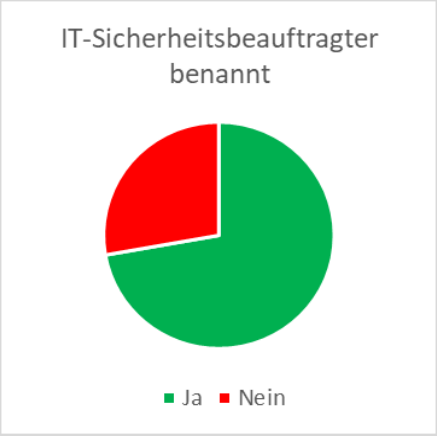
Grundrecht auf freie ungestörte Religionsausübung gemäß Art. 4 Grundgesetz (GG) und dem Selbstbestimmungsrecht der Kirchen gemäß Art. 140 GG in Verbindung mit Art. 137 und Art. 141 Weimarer Reichsverfassung. Grundsätzlich empfehlen wir immer die **Einholung einer Einwilligung** der Patientinnen und Patienten in die Übermittlung der Kontaktdaten an die Krankenhausseelsorge. Die Weitergabe von Behandlungsdaten (insbesondere einer Diagnose) ist grundsätzlich unzulässig. Es gibt aber Fälle, in denen eine gesetzliche Regelung auf landeskirchlicher Ebene in den Datenschutzdurchführungsverordnungen zur Übermittlung von Daten zu Zwecken der Krankenhausseelsorge getroffen worden sind. In diesen Fällen liegt auch ohne das Einholen einer Einwilligung kein Datenschutzverstoß vor, wenn bei Angabe der Konfession die Kontaktdaten der Patientinnen und Patienten übermittelt werden. Die Patientinnen und Patienten sollten aber bei der Aufnahme darauf hingewiesen werden, dass sie der Übermittlung jederzeit widersprechen können. Im Rahmen der Prüfung konnten wir feststellen, dass die Offenlegung größtenteils auf Einwilligungsbasis durchgeführt wird.

Knapp ein Drittel der befragten Krankenhäuser betreiben **interne Forschung** mit den Daten ihrer Patientinnen und Patienten. Seit Einführung der Datenschutzgrundverordnung existiert ein **datenschutzrechtliches Forschungsprivileg**, das sich auch im EKD-Datenschutzgesetz wiederfindet. Damit ist es Einrichtungen grundsätzlich möglich, mit den Daten ihrer Patientinnen und Patienten zu forschen, auch wenn die Gesundheitsdaten ursprünglich nicht für diesen Zweck erhoben wurden. **Externe Forschung** liegt hingegen vor, wenn Dritte als Partner in den Projekten in die Forschung eingebunden werden. Hierzu zählen **klassischerweise Universitäten oder Pharmaunternehmen**. In diesen Fällen besteht regelmäßig ein Interesse an den Gesundheitsdaten der Krankenhäuser, die - soweit sie Personenbezug aufweisen - grundsätzlich nur auf Basis einer **Einwilligung** Teil solcher Forschungsprojekte werden können. Im Rahmen unserer Prüfung konnten wir feststellen, dass zwei Drittel der Häuser an solchen Forschungsprojekten teilnehmen.

Fragen aus dem technischen Umfeld

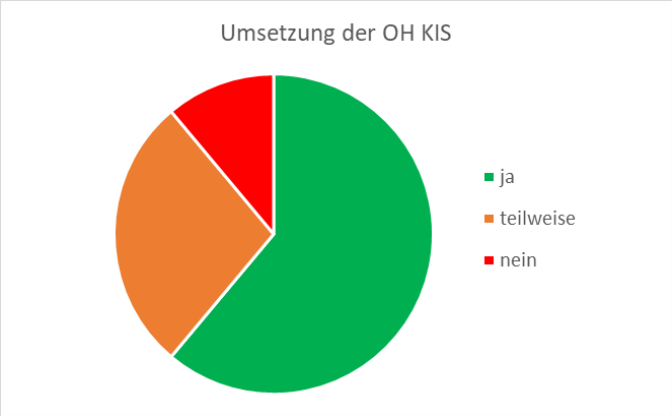
IT-Organisation

Für alle Krankenhäuser gelten besondere Anforderungen an die **IT-Sicherheit**. Diese leiten sich für die größeren Häuser aus den IT-Sicherheitsgesetzen aus den Jahren 2015 und 2021 ab, in denen Mindeststandards für Einrichtungen der kritischen Infrastruktur festgelegt wurden. Darüber hinaus verpflichtet der „Branchenspezifische Sicherheitsstandard (B3S)“, erarbeitet durch die Deutsche Krankenhausgesellschaft und ratifiziert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), alle Krankenhäuser zu vergleichbaren Maßnahmen, beispielsweise der Benennung eines Informations-Sicherheitsbeauftragten, der Dokumentation von Sicherheitsvorfällen und regelmäßigen Auditierungen. Diese Anforderungen sind grundsätzlich bekannt und werden umgesetzt. Defizite gab es im Reporting: Auditberichte waren in Einzelfällen nicht verfügbar oder veraltet. In mehreren Fällen war zum Zeitpunkt der Befragung (noch) kein IT-Sicherheitsbeauftragter benannt und oder es lag kein aktueller Audit-Bericht vor.



Krankenhaus-Informationssystem (KIS)

Ein Großteil unserer Fragen bezog sich auf den Einsatz des verwendeten **KIS**, welches in den Krankenhäusern für die **Verarbeitung von Patientendaten** - aber auch von Daten der Mitarbeitenden - eine zentrale Rolle spielt. Neben dem KIS sind oft noch kaufmännische Systeme (Buchhaltung) und Human Resource (HR)-Systeme für die Personalwirtschaft im Einsatz, die von uns im Rahmen dieser Prüfung nicht betrachtet wurden. Aufgrund der zentralen Bedeutung des KIS für die operative Umsetzung und Gewährleistung von IT-Sicherheit und Datenschutz im Krankenhaus haben die Deutsche Krankenhausgesellschaft und die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) im Jahr 2014 eine **Orientierungshilfe zur Auswahl und datenschutzkonformen Einstellung und Betrieb von Krankenhausinformationssystemen (OH KIS)** erstellt. Auch die Kirchen wurden bei der Entstehung der Orientierungshilfe beteiligt. Wichtige Abschnitte der OH KIS widmen sich der Definition und Zuweisung von Berechtigungen (Rollen), der Protokollierung von Aktivitäten der Anwender und dem Löschen von Daten nach Zweckerfüllung.



Berechtigungskonzepte

Alle Krankenhäuser weisen den Mitarbeitenden im KIS eine Menge von **Einzelberechtigungen** („Rolle“) zu, die auf den spezifischen Aufgaben basieren. So gibt es z. B. Rollen für Pflegende auf den Stationen, für Ärztinnen und Ärzte, für Verwaltungskräfte und für ambulante Dienste. Die Anlage von Benutzern im KIS und die Zuweisung der Rollen wird immer transparent dokumentiert.

Die OH KIS fordert eine Rollen-Struktur, die sich aus **funktionalen Rollen** (Beruf/Aufgabe des Nutzenden, siehe oben) **<u>und</u> strukturellen Rollen** zusammensetzt. Strukturelle Rollen bilden die organisatorische Struktur des Krankenhauses (z. B. die Untergliederung in Kliniken und Stationen) ab und sollen die Zugriffe der Nutzenden auf Daten des „eigenen“ Bereiches begrenzen.

Während die Zuweisung funktionaler Rollen keine Probleme macht, ist die Ausprägung und die Handhabung struktureller Rollen oft mangelhaft. Viele Krankenhäuser geben an, dass durch die geforderte Agilität, das häufige Verschieben von Personal zwischen den Krankenhausbereichen und oft fachmedizin-übergreifende Behandlungen ein **effektives Management der strukturellen Berechtigungen nicht oder kaum möglich** sei. Das führt leider oft dazu, dass in der Praxis weitreichende Berechtigungen zur Einsicht in Patientendaten vergeben sind.

Immerhin konnte bei allen Nachfragen und Vor-Ort-Prüfungen zu diesem Thema nachgewiesen werden, dass zumindest für bestimmte Patientengruppen mit besonderem Schutzbedarf (z. B. Patienten auf psychiatrischen Stationen oder Mitarbeitende des Hauses, die als Patienten behandelt werden) Mechanismen eingerichtet waren, die den Zugriff auf die Daten dieser Personengruppen eingrenzen.

Um die Aufklärung möglicher Datenschutzverstöße zu ermöglichen, fordert die OH KIS eine **Auswertemöglichkeit der bestehenden Berechtigungen** zum aktuellen Abfrage-Zeitpunkt. Diese Anforderung wird von allen Krankenhäusern erfüllt. Allerdings ist nur ein kleinerer Teil der Häuser in der Lage, eine solche Auswertung auch für **beliebige Zeitpunkte in der Vergangenheit** (historischer Berechtigungsreport) durchzuführen. Hinzu kommt, dass solche Auswertungen oft nicht im KIS-Standardumfang bereitgestellt werden, sondern durch die Krankenhaus-IT per Datenbank-Abfrage selbst programmiert werden müssen.

Ein weiterer Schwachpunkt in einigen Häusern ist die **Berechtigungs-Spezifikation für neue Nutzende** durch die Fachabteilungen. Hier wird oft „genau wie Kollegin/Kollege XY“ formuliert, statt aus einer vorgegebenen Menge an Optionen stellengenau auszuwählen. Die Möglichkeit, Berechtigungen zeitlich zu begrenzen, wird kaum genutzt. Ein regelmäßiges Review der vorhandenen Benutzerkonten mit deren Berechtigungen durch die Fachvorgesetzten findet kaum statt.

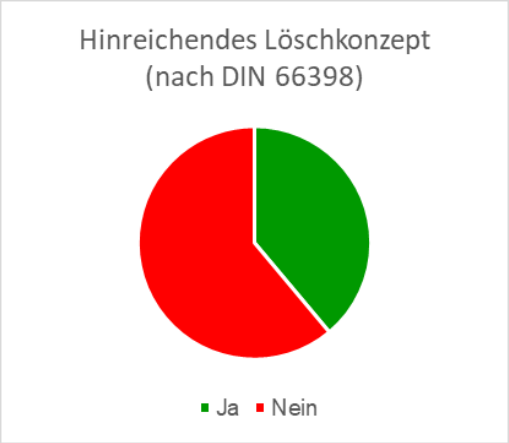
Protokollierung

Alle im Rahmen unserer Prüfung vorgefundenen Krankenhaus-Informationssysteme ermöglichen – wie von der OH KIS gefordert – die **Protokollierung aller lesenden und schreibenden Zugriffe** auf die Patientendaten und Fallakten. Das wird von den geprüften Häusern in angemessenem Umfang genutzt, wodurch sich potentielle Datenschutzverstöße gut aufklären lassen und auch der Auskunftsanspruch der Betroffenen erfüllbar wird.

Die OH KIS fordert neben der Möglichkeit der anlassbezogenen Prüfung der Protokolle auf unberechtigte Verarbeitungen aber auch die Einrichtung von **stichprobenartigen Kontrollen**. Leider mussten wir feststellen, dass nur sehr wenige Krankenhäuser ein Verfahren etabliert haben, das unter Wahrung der Mitarbeiterrechte und datenschutzkonform die Protokolldaten regelmäßig anlasslos zumindest stichprobenartig auswertet. Hier sehen wir erheblichen **Handlungsbedarf**.

Löschen und „Archivieren“

Nach eigenen Angaben verfügen nur etwas mehr als die Hälfte der befragten Krankenhäuser über ein **Konzept zur Löschung von Daten**, dass auch in allen Systemen des Hauses umsetzbar ist und konsequent umgesetzt wird. In mehreren Fällen haben wir festgestellt, dass die vorgelegten Löschkonzepte nicht den Anforderungen der **DIN 66398** entsprechen, weil z. B. die Einteilung der Daten in Löschklassen nicht vollständig erfolgte oder die konkreten Löschverfahren mit der eingesetzten Technik und den Verantwortlichkeiten nicht beschrieben wurden.



In vielen Beschreibungen schließt sich an die operative Nutzungs- und die Aufbewahrungszeit eine „Archivierung“ an, wobei mit diesem Begriff meistens die Ablage in einer speziellen Speichertechnik (oft bei einem Dienstleister) gemeint ist. Eine wirkliche Archivierung, also die Übergabe an ein anerkanntes kirchliches oder diakonisches Archiv zum Zweck der dauerhaften Bewahrung und zukünftigen wissenschaftlichen Forschung und Aufarbeitung hat kaum ein Haus im Blickfeld.

In keinem Löschkonzept konnten wir Hinweise auf die archivarische Zuständigkeit oder mit einem anerkannten Archiv getroffene Vereinbarungen zur Andienung und Übergabe von Daten finden. Auch hier besteht dringender Handlungsbedarf.

Zusammenfassung

Die 20 evangelischen Krankenhäuser, die wir im Zuge der Schwerpunktprüfung befragt haben, können erwartungsgemäß ein **gutes Datenschutzniveau** nachweisen. Der hohe Grad der Digitalisierung macht sich hier positiv bemerkbar und ist auch hilfreich bei der Erfüllung der Rechenschaftspflichten. Das gilt insbesondere dann, wenn alle Daten und Einwilligungen im gleichen System dokumentiert werden. Bei der Umsetzung des rechtlichen und technischen Datenschutzes hilft eine konsequente Orientierung am Branchenspezifischen Sicherheitsstandard (B3S) und die Anwendung der OH KIS.

Defizite wurden vereinzelt in den Bereichen der Berechtigungsvergabe und der Auswertung von Systemprotokollen festgestellt. Auch die Vertretung der örtlich Beauftragten für den Datenschutz muss in manchen Häusern noch konkret geregelt werden. Nur wenige Krankenhäuser verfügen bisher über ein vollständiges Löschkonzept für personenbezogene Daten und setzten dieses auch in der Praxis um. Hier besteht noch Handlungsbedarf.

Abschließend möchten wir an dieser Stelle den geprüften Krankenhäusern für Ihre Kooperationsbereitschaft und die gute Zusammenarbeit danken. Ebenfalls möchten wir uns bei den Diakonischen Landesverbänden bedanken, die das gesamte Verfahren begleitet und unterstützt haben.

Ausblick

Die nächste Schwerpunktprüfung findet im Bereich der **kirchlichen Verwaltung** mit einem Schwerpunkt auf dem **Umgang mit Meldedaten** im Zeitraum 2025/2026 statt und ist bereits in der Vorbereitung. Genauere Informationen zum Ablauf und zum Zeithorizont der Prüfung werden zu gegebener Zeit den Landeskirchen mitgeteilt.

Hannover im Juni 2025