Wartung und Fernwartung von Datenverarbeitungssystemen im medizinischen Krankenhausbereich

Auffassung des Sächsischen Datenschutzbeauftragten

Der Sächsische Datenschutzbeauftragte hat der Sächsischen Landesärztekammer mit Schreiben vom 25.11.1998 zu der Problematik Wartung und Fernwartung von Datenverarbeitungssystemen im medizinischen Krankenhausbereich seine Auffassung mitgeteilt. Dieses Schreiben veröffentlichen wir nachfolgend mit Genehmigung des Sächsischen Datenschutzbeauftragten.

„Wartung und Fernwartung im medizinischen Krankenhausbereich
Schreiben des Sächsischen Datenschutzbeauftragten vom 25.11.1998

Sehr geehrte Damen und Herren,

heute wird in der modernen Medizin eine Vielzahl technischer Geräte eingesetzt, deren Wartung durch Klinikpersonal wegen der dafür benötigten Spezialkenntnisse nicht mehr möglich sein dürfte. Diese Geräte speichern und verarbeiten zum Teil hochsensible Patientendaten, die unter dem Schutz der ärztlichen Schweigepflicht stehen. Auf den Rechnern ist meist auch noch Fremdsoftware im Einsatz, so daß bei Störungen sowie bei in der Hard- oder Software auftretenden Fehlern der Hersteller eingeschaltet werden muß. Das kann vor Ort geschehen, meist jedoch im Rahmen des Teleservice, also in Form einer Ferndiagnose und -wartung. Bei der Hardwarewartung wird in der Regel nur auf bestimmte Statusinformationen in eigens dafür eingerichteten Diagnosedateien zugegriffen, die keine personenbezogenen Daten enthalten.

Die moderne Programmiertechnik und die mächtigen Programmsysteme machen es für den Anwender nahezu unmöglich, Programmeingriffe vorzunehmen, Fehler selbst zu lokalisieren oder gar zu beheben. Schließlich sind die DV-Systeme so komplex geworden, daß klinikeigenes Personal allenfalls die Einweisung in die Programmbenutzung vornehmen kann. Eine Einweisung in andere Funktionen scheitert auch an den zur Verfügung stehenden Ressourcen (Anzahl und know-how der DV-Mitarbeiter). Aus diesen Gründen sind die Wartung und Fernwartung der Hardware und Software durch den Hardwarehersteller bzw. durch das Softwarehaus für ein Krankenhaus notwendig geworden.
Bei vielen DV-Systemen kann die Fehlerdiagnose und -behebung mit einer Offenbarung geschützter Patientendaten verbunden sein. Eine verschlüsselte Abspeicherung der identifizierenden Merkmale scheidet aus verschiedenen Gründen aus, nämlich, weil der Wartende bei der Fehlerdiagnose in den Anwendermodus gehen muß und der Anwender mit verschlüsselten Daten nicht arbeiten kann oder weil eine Konsistenzprüfung der Datenbank mit verschlüsselten Daten nicht möglich ist. Hinzu kommt, daß viele Wartungsarbeiten auch für den Anwender nicht transparent sind, weil entweder das DV-know-how fehlt oder keine Überwachungsmöglichkeiten vorhanden sind.

Da Krankenhäuser und Ärzte wegen ihrer Verpflichtung für eine optimale Versorgung ihrer Patienten vom Einsatz solcher Fremdsysteme nicht Abstand nehmen können, müssen neben rechtlichen vor allem technische Maßnahmen ergriffen werden, die erkennbar machen, wann zu welchem Zweck auf welche Daten durch Dritte zugegriffen wurde.

Grundsätzlich sollte die Fernwartung von DV-Systemen, die mit Patientendaten arbeiten, nur in begründeten Ausnahmefällen stattfinden. Bei einer Wartung vor Ort ist darauf zu achten, daß die Datenträger, die das Fremdpersonal bei der Wartung benützt, keine personenbezogenen Daten des Krankenhauses enthalten.

Technische Maßnahmen
• Arbeiten am Testsystem

Soweit wie möglich sollen Externe nur an solchen Systemen arbeiten, in denen entweder nur signifikante Testfälle (ohne Bezug auf eine konkrete Person) oder anonymisierte Patientendaten gespeichert sind.

• Arbeiten im Produktionssystem

Ist für eine Fehlerdiagnose und -behebung der Zugriff auf das Produktionssystem erforderlich, sollten folgende Maßnahmen ergriffen werden:

- Verbindungsaufbau
Bei der Fernwartung ist die Verbindung oder die Freischaltung (nach einem Authentifikationsprozeß) stets vom Anwender aus aufzubauen (Call-Back-Verfahren) oder freizugeben, damit sichergestellt ist, daß keine unbefugten Einwählversuche stattfinden können. Nach Abschluß der Wartungsarbeiten ist diese Verbindung wieder zu deaktivieren.

- Zugriff
Vom Anwender sind der Wartung/Fernwartung nur solche Zugriffsmöglichkeiten zu eröffnen, die für die Fehlerbehebung unbedingt erforderlich sind. Diese Zugriffe sind unter einer extra dafür eingerichteten Kennung mit einem Paßwort, das nur einmal verwendet werden kann, durchzuführen. Es ist ferner darauf zu achten, daß im Rahmen der Wartung bzw. Fernwartung keine Funktionen freigeschaltet werden, die eine Übertragung oder Auswertung von Anwenderdatenbeständen zulassen. Befindet sich der Rechner, an dem Fernwartung durchgeführt wird, in einem internen Netz, ist die Verbindung zu diesem Netz zu lösen.

- Vieraugenprinzip
Alle Aktivitäten der Wartung bzw. Fernwartung muß ein sachverständiger Mitarbeiter des Krankenhauses am Bildschirm verfolgen können. Im Zweifelsfalle muß dieser Mitarbeiter diese Aktivitäten auch abbrechen können (bei manchen Systemen ist das nur eingeschränkt möglich, hier müssen stärkere Protokollierungsvorschriften greifen).

- Protokollierung
In einem Protokoll sind alle Aktivitäten

der Wartung bzw. Fernwartung aufzuzeichnen. Bei besonders kritischen Aktionen ist der gesamte Dialog zu protokollieren, damit später erkennbar wird, auf welche Daten zugegriffen wurde. So gibt es beispielsweise Systeme, die eine ganze Sitzung (alle Aktivitäten am Bildschirm) gleichsam wie in einem Video aufzeichnen können.

- Vertraulichkeit auf dem Übertragungswege

Zur Sicherung der Vertraulichkeit der übertragenen Daten auf dem Übertragungswege kann es erforderlich sein, daß die Daten verschlüsselt werden. Es ist jedoch darauf zu achten, daß die Protokollierung vor Ort unverschlüsselt erfolgt. Nur so ist eine effektive Kontrolle durch den Anwender gewährleistet.

Organisatorische Maßnahmen

Im Interesse klarer Verhältnisse für Patienten und Krankenhäuser bei Fremdwartung schlage ich vor, die Einwilligung des Patienten über eine Klausel im Krankenhaus-Aufnahmevertrag einzuholen. Durch eine wirksame Einwilligung können die mit der Fremdwartung verbundenen strafrechtlichen Risiken für die Krankenhäuser minimiert werden. Voraussetzung dafür, daß den Patienten eine Klausel zur Fremdwartung im Aufnahmevertrag zugemutet werden kann, ist jedoch, daß die Offenbarung von Patientendaten an die Wartungsfirma auf das unumgängliche Maß eingeschränkt wird. D. h., daß in der Praxis alle technischen und organisatorischen Sicherungsmöglichkeiten zu aktivieren sind, damit Patientendaten nur dann zur Kenntnis der Wartungsfirma gelangen, wenn mit vertretbarem Aufwand keine andere Lösung möglich ist.

Die Wartung und vor allem die Fernwartung sind auf eine vertragliche Grundlage zu stellen, in der das Wartungsunternehmen explizit zur Verschwiegenheit verpflichtet wird. Für Zuwiderhandlungen sind **empfindliche** Vertragsstrafen vorzusehen. Die Unternehmen müssen Erklärungen über die Zuverlässigkeit ihres Wartungspersonals abgeben. Unter Umständen empfiehlt es sich, Führungszeugnisse nach dem BZRG zu verlangen.

Die externen Mitarbeiter müssen der Klinik oder dem Krankenhaus namentlich benannt werden. Dieser Personenkreis soll aber überschaubar bleiben und möglichst wenig wechseln.

Bei lokaler Wartung ist in einem Logbuch Zeitpunkt, Ursache und Name dessen, der die Wartung durchführt, festzuhalten.
Schließlich sollte die Wartung und Fernwartung nur dann durchgeführt werden, wenn sichergestellt ist, daß ausreichender eigener Sachverstand für die Beurteilung der externen Aktivitäten vorhanden ist.

Für alle Wartungs- und Fernwartungsaktivitäten ist ein Logbuch zu führen. Aus den Einträgen muß der Grund der Wartung, der Zeitpunkt und die die Wartung durchführende Person sowie die Wartungsaktivitäten, insbesondere ob auf den Echtdatenbestand zugegriffen werden mußte, erkennbar sein.

Ich lege großen Wert darauf, dem SMS ein mit Ihnen abgestimmtes Konzept mit der Maßgabe zur Verfügung zu stellen, den sächsischen Krankenhäusern einheitliche Vorgaben für die Vertragsgestaltung und das „handling" der Fernwartung an die Hand zu geben. Deshalb bin ich für Ihre rechtliche und fachliche Einschätzung meiner Ausführungen sowie für Ergänzungs- und Verbesserungsvorschläge dankbar. Dabei bitte ich zu berücksichtigen, daß meine bisherige Sichtweise geprägt war von der Überzeugung, bei der Wartung/Fernwartung von Datenverarbeitungsanlagen mit Patientendaten sei § 33 Abs. 10 SächsKHG einschlägig, was sich nach neuerlicher rechtlicher Würdigung nicht mehr aufrechterhalten läßt. Da Wartung/Fernwartung sich nicht auf den **Informationsgehalt** von Datenfeldern bezieht, liegt nach meinem Dafürhalten auch keine „Verarbeitung" (im Auftrag) i. S. v. § 33 Abs. 10 SächsKHG vor (Wartung/Fernwartung bedarf daher auch keiner vorherigen Zustimmung durch das Regierungspräsidium). Vielmehr konzentriert sich das Interesse des Wartungspersonals üblicherweise ausschließlich darauf, Fehler an Hard- und Software zu beheben. Selbst wenn zur Fehlerbeseitigung im Einzelfall Patientendaten zur Verfügung gestellt werden müßten und dabei ggf. offenbar würden, ist das kein Datenverarbeitungsschritt, sondern eine unabdingbare „Nebenfolge", die wohl in Kauf genommen werden muß.

Gleichwohl darf die Frage der Zulässigkeit der Offenbarung von Patientendaten im Zuge der Wartung/Fernwartung unter Aufgabe des bisherigen Standpunktes zur Anwendbarkeit des § 33 Abs. 10 SächsKHG nicht vernachlässigt werden. Die seinerzeit ins Leben gerufene Arbeitsgruppe zum Thema Wartung/Fernwartung in Krankenhäusern halte ich in der bisherigen Besetzung aber für nicht mehr erforderlich.

Im Auftrag
gez. Rokoß
Ministerialrat"

Dienstanschrift des Verfassers:

Der Sächsische Datenschutzbeauftragte
Postfach 120 905, 01008 Dresden
Tel.: (0351) 49 35-4 15

Sofern Sie Rückfragen zu diesem Thema haben, steht Ihnen selbstverständlich auch die Juristische Geschäftsführerin, Frau Glowik, Tel.-Nr. (0351) 8 26 74 21, zur Verfügung.

Ass. Iris Glowik
Juristische Geschäftsführerin