Bildung von Vertrauen im Medizinbereich durch Datenschutz-Gütesiegel und -audit

Barbara Körffer
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

1 Die Notwendigkeit der Vertrauensbildung im Medizinbereich

Zur Unterstützung und Verbesserung von Behandlungs- und Organisationsabläufen im Medizinbereich ist der Einsatz moderner Technik und effizienter Verfahren von erheblicher Bedeutung. Ziel solcher Bestrebungen ist es meist, Daten über die Patienten zentral zusammen zu führen, um eine umfassende Informationsgrundlage für die Behandlung der Patienten den Beteiligten zur Verfügung zu stellen und so Fehl- oder Doppelbehandlungen zu vermeiden. In anderen Fällen sind fehlende Kapazitäten Anlass dafür, die Verarbeitung von Patientendaten in kompetente Hände zu geben, die diese „outgesourcten" Verfahren fachmännisch und effizient erledigen. All diesen Bestrebungen wohnt aber stets das gleiche Hindernis inne: Fehlendes Vertrauen in den sicheren Umgang mit den Daten, die einem technischen System oder einem fremden Dienstleister überlassen werden. Hierbei geht es um hochsensible Daten, die zu einem der persönlichsten Bereiche der Menschen gehören, nämlich seiner Gesundheit. So wenig Patienten Daten über ihre Gesundheit preisgeben möchten, so begehrt ist ihre Kenntnis auf der anderen Seite. Geraten Gesundheitsdaten in falsche Hände, etwa in die des Arbeitgebers oder der Versicherung, drohen dem Betroffenen erhebliche Nachteile. Kein Wunder also, dass moderner Technik oder spezialisierten Dienstleistern insbesondere zur elektronischen Verarbeitung von Patientendaten häufig Skepsis entgegengebracht wird. Die Frage, ob die hochsensiblen Daten in diesen Systemen nach den strengen Anforderungen des Patientengeheimnisses verarbeitet werden, wird an dieser Stelle häufig gestellt. Die Beantwortung ist indessen oftmals nicht leicht. Sowohl die technischen Systeme als auch die rechtlichen Anforderungen sind komplex. Häufig ist der Rat von Experten gefragt.

Diesen Expertenrat in einfacher Form und verständlich der Öffentlichkeit zu kommunizieren und damit Vertrauen in Datenverarbeitungsverfahren oder -produkte zu schaffen, die den Anforderungen an Datenschutz und Datensicherheit entsprechen, ist Anliegen der Instrumente Datenschutzaudit und Datenschutzgütesiegel. In Form eines Gütezeichens wird dem Anwender, dem Betroffenen oder der interessierten Öffentlichkeit signalisiert, dass ein Verfahren oder ein Produkt durch eine unabhängige und kompetente öffentliche Stelle im Hinblick auf Datenschutz und Datensicherheit geprüft wurde und die entsprechenden Anforderungen erfüllt. Nachvollziehbar und nachprüfbar wird die Aussage dieses Gütezeichens durch eine Bewertung des Verfahrens oder Produkts, die durch Veröffentlichung dem interessierten Kreis zugänglich gemacht wird und verbleibende Fragen oder Zweifel an dem Verfahren oder Produkt beantwortet bzw. beseitigt.

2 Zertifizierung und Auditierung nach dem Landesdatenschutzgesetz Schleswig-Holstein

Das Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) sieht nach seiner Novellierung im Jahr 2000 zur Verbesserung des Datenschutzes die Instrumente des Datenschutz-Audits für Behörden und des Gütesiegels für IT-Produkte vor. Die entsprechenden Regelungen zur Umsetzung dieser Instrumente sind im Folgejahr erlassen worden[1] und somit konnten beide Verfahren in den Jahren 2001 bzw. 2002 in die Praxis eingeführt werden. Damit ist Schleswig-Holstein das bislang einzige Bundesland, das im Datenschutz Audit und Gütesiegel auf gesetzlicher Grundlage anbietet.

Da der Landesgesetzgeber eine Gesetzgebungskompetenz nur für den Bereich der Landesbehörden hat, knüpfen zwangsläufig auch die Elemente des Datenschutzaudits und des Gütesiegels an die Datenverarbeitung in öffentlichen Stellen in Schleswig-Holstein an. Aus diesem Grund ist ein Datenschutzaudit nach § 43 Abs. 2 LDSG SH nur für öffentliche Stellen in Schleswig-Holstein möglich. Privaten Unternehmen ist die Auditierung durch das Unabhängige Landeszentrum für Datenschutz (ULD) nach dem LDSG SH grundsätzlich nicht möglich, wenngleich nach einem solchen Verfahren eine nicht geringe Nachfrage besteht. Die Regelungskompetenz für Audits im Privatbereich liegt beim Bundesgesetzgeber, der zwar in § 9a BDSG bereits die Grundlage für solche Audits und Produktzertifizierungen geschaffen hat, mit dem Erlass des zur Umsetzung erforderlichen Ausführungsgesetzes jedoch auf sich warten lässt. In der Zwischenzeit kann das schleswig-holsteinische Behördenaudit zumindest indirekt zur Auditierung privater Unternehmen eingesetzt werden. Von dieser Möglichkeit ist in der Vergangenheit Gebrauch gemacht worden, indem ein

Autorin: Barbara Körffer
Titel: Bildung von Vertrauen im Medizinbereich durch Datenschutz-Gütesiegel und -audit
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2005
Seite: 276-280

privates Unternehmen eine Kooperation mit einer öffentlichen Stelle in Schleswig-Holstein eingegangen ist. Die öffentliche Stelle hat im Auftrag des Unternehmens ein Datenschutzkonzept erstellt, das vom ULD auditiert und von dem Unternehmen eingesetzt wurde. Sowohl der öffentlichen Stelle als auch dem Unternehmen ist es auf diese Weise möglich, mit dem Datenschutzaudit zu werben.

Einen Schritt weiter als das Datenschutzaudit geht das Datenschutz-Gütesiegel. Es dient nach seiner gesetzlichen Verankerung in § 4 Abs. 2 LDSG SH primär als Empfehlung an öffentliche Stellen in Schleswig-Holstein, die solche IT-Produkte, die mit den Vorschriften über Datenschutz und Datensicherheit vereinbar sind, vorrangig einsetzen sollen. Das Gütesiegel kennzeichnet Produkte, die diese Voraussetzungen nach einem förmlichen Verfahren erfüllen. Es wird daher direkt für ein Produkt eines in der Regel privaten Herstellers verliehen, der mit dem Gütesiegel über den Bereich der schleswig-holsteinischen Verwaltung auch im Privatkundengeschäft werben kann. Das Gütesiegel ist keineswegs an den tatsächlichen Einsatz in der schleswig-holsteinischen Verwaltung geknüpft. Es genügt, wenn das zu zertifizierende Produkt geeignet ist, dort eingesetzt zu werden. Die Zertifizierung ist weder an einen Sitz des Herstellers noch einen Vertrieb des Produkts in Schleswig-Holstein geknüpft.

a) Verfahren zur Verleihung des Gütesiegels

Gemäß § 4 Abs. 2 LDSG SH sind öffentliche Stellen in Schleswig-Holstein gehalten, solche Produkte vorrangig einzusetzen, deren Vereinbarkeit mit den Vorschriften über Datenschutz und Datensicherheit in einem förmlichen Verfahren bestätigt wurde. Das ULD verleiht auf dieser Rechtsgrundlage, die in der Gütesiegel-Verordnung (DSAVO) näher ausgestaltet wurde, Gütesiegel für IT-Produkte als Empfehlung für öffentliche Stellen in Schleswig-Holstein.

Ein Gütesiegel kann für jedes IT-Produkt – sowohl Hard- und Software als auch ein automatisiertes Verfahren – erlangt werden. Klassisches Anwendungsfeld für Gütesiegel im Medizinbereich sind daher Software-Produkte zur Verarbeitung von Patientendaten, z. B. Arztpraxissoftware. Über den Bereich der automatisierten Verfahren, die ebenfalls als zertifizierungsfähiges Produkt gelten, wird auch der Bereich der Dienstleistungen für ein Gütesiegel eröffnet. Unter automatisierten Verfahren versteht die entsprechende Verordnung „Arbeitsabläufe mit Hilfe von informationstechnischen Geräten, Programmen und automatisierten Dateien“[2]. Anwendungsbereich dieser Alternative ist im Wesentlichen der gesamte Bereich der Datenverarbeitung im Auftrag, des so genannten Outsourcings, das im Medizinbereich eine zunehmende Rolle spielt. Bereits als „automatisiertes Verfahren“ zertifiziert wurde vom ULD ein Aktenvernichtungsunternehmen sowie Dienstleister, die die elektronische Archivierung von Patientendaten anbieten.

Das Zertifizierungsverfahren vollzieht sich im Wesentlichen in zwei Schritten: Zunächst wird das zu zertifizierende Produkt durch einen unabhängigen Sachverständigen begutachtet. Hierzu schließt der Produkthersteller einen privaten Begutachtungsvertrag mit einem Sachverständigen. Die Begutachtung wird durch Sachverständige vorgenommen, die beim ULD in einem gesonderten Verfahren akkreditiert wurden.

Der zweite Verfahrensschritt beginnt nach erfolgreichem Abschluss der Begutachtung. Der Hersteller des Produkts stellt beim ULD einen Antrag auf Zertifizierung des begutachteten Produkts, dem das vom Sachverständigen erstellte Gutachten beigefügt wird. Das ULD überprüft, ob das Gutachten nachvollziehbar und schlüssig ist. Außerdem können ergänzende Angaben und die Vorlage des Produkts bei Bedarf vom ULD zusätzlich angefordert werden.

Nach erfolgreicher Prüfung verleiht das ULD das Gütesiegel. Dies gilt befristet für den Zeitraum von zwei Jahren. Des Weiteren gilt es nur für die Produktversion, die der Begutachtung im Gütesiegelverfahren zu Grunde lag. Wird das Produkt gegenüber der geprüften Version mehr als unerheblich verändert, ist für die neue Version das Gütesiegel nicht mehr gültig. In beiden Fällen – Zeitablauf und Produktänderung – ist eine Rezertifizierung erforderlich, um das Gütesiegel weiterhin nutzen zu können. In der Regel wird das Zertifizierungsverfahren – abhängig von den erfolgten Änderungen – unter vereinfachten Bedingungen durchgeführt werden können.

Die zertifizierten Produkte werden in ein beim ULD geführtes Register eingetragen, das ebenso wie das vom Sachverständigen erstellte Kurzgutachten über die Homepage des ULD veröffentlicht wird. Auf diese Weise wird eine für den Anwender wichtige Transparenz hergestellt. Anhand des Kurzgutachtens des unabhängigen Sachverständigen können sich die Anwender darüber unterrichten, aus welchen Gründen und in welcher Weise das Produkt Datenschutz konform einsetzbar ist. Nicht zuletzt diese Transparenz ist ein entscheidender Faktor, um Vertrauen des Anwenders und ebenfalls der Betroffenen, d. h. im Gesundheitsbereich der Patienten, in das Produkt zu schaffen. Nach der Gütesiegelverordnung ist es dem Hersteller ebenfalls ermöglicht, ein erhaltenes Gütesiegel in der Werbung für sein Produkt einzusetzen. Adressaten der Produktwerbung können nicht nur die Anwender des Produkts sein, sondern ebenfalls die von der Datenverarbeitung betroffenen Patienten und die Öffentlichkeit, die gerade im Medizinbereich technischen Neuerungen zur Verarbeitung von Patientendaten häufig skeptisch gegenüber steht.

b) Ablauf des Audit-Verfahrens beim ULD

Das Datenschutzaudit kann für sämtliche Bereiche einer öffentlichen Stelle erlangt werden, in denen Personen bezogene Daten verarbeitet werden. Wegen der Beschränkung auf öffentliche Stellen in Schleswig-Holstein richtet sich dieses Verfahren im Medizinbereich primär an öffentlich-rechtlich organisierte Einrichtungen im Gesundheitswesen, z. B. öffentliche Krankenhäuser, Gesundheitsämter, Unternehmen der gesetzlichen Krankenversicherungen oder Universitäten. Mittelbar können wie bereits erwähnt, durch eine Kooperation mit öffentlichen Stellen auch private Unternehmen an einem Auditverfahren teilnehmen und das Audit zu eigenen Zwecken nutzen.

Das Spektrum möglicher Auditgegenstände reicht von einem einzelnen

Verfahren zur Verarbeitung personenbezogener Daten über bestimmte abgrenzbare Teilbereiche der Daten verarbeitenden Stelle – etwa eine bestimmte Station eines Krankenhauses – bis hin zur gesamten Verarbeitung Personen bezogener Daten in der öffentlichen Stelle.

Um das Auditzeichen zu erlangen, führen die Daten verarbeitende Stelle und das ULD ein Auditverfahren durch, dessen Ablauf durch Anwendungsbestimmungen des ULD geregelt ist. In diesem Verfahren sind von beiden Seiten die folgenden Schritte durchzuführen:

- Bestandsaufnahme
- Festlegung der Datenschutzziele
- Einrichtung eines Datenschutzmanagementsystems
- Begutachtung der Datenschutzerklärung durch das ULD
- Verleihung des Auditzeichens

Die ersten drei Schritte werden von der öffentlichen Stelle vorgenommen. In einer so genannten Datenschutzerklärung dokumentiert die Daten verarbeitende Stelle diese Schritte zusammenfassend und übergibt diese Dokumentation des ULD zur Begutachtung, welches bei positivem Ausgang das Datenschutzauditzeichen verleiht.

Das ULD fasst das Ergebnis seiner Mitwirkung am Verfahren in einem Kurzgutachten zusammen. Dieses enthält zum einen eine Zusammenfassung der von der Behörde erstellten Datenschutzerklärung und zum anderen die wesentlichen Gründe des ULD für die Verleihung des Auditzeichens. Das ULD veröffentlicht das Kurzgutachten zusammen mit der Auditverleihung auf seiner Homepage. Auf diese Weise können sich Betroffene sowie die interessierte Öffentlichkeit darüber informieren, wie in den auditierten Verfahren personenbezogene Daten verarbeitet und welche Maßnahmen zum Schutz dieser Daten ergriffen wurden. Hierdurch wird wie beim Gütesiegel ein hohes Maß an Transparenz und somit auch an Vergleichbarkeit zwischen verschiedenen öffentlichen Stellen erreicht. Den Betroffenen, wie etwa den Patienten, wird es durch diese Informationen ermöglicht, selbst zu überprüfen, welche Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die öffentliche Stelle festgelegt hat und ob die von der auditierten Stelle selbst auferlegten Datenschutzziele in der Praxis erreicht werden.

3 Rechtslage im übrigen Bundesgebiet

3.1 Gesetzliche Situation

Bundesweit ist Schleswig-Holstein das einzige Land, das bereits Ausführungsbestimmungen zur Regelung von Audit- und Gütesiegelverfahren erlassen und diese Verfahren in die Praxis umgesetzt hat. Initiativen in die gleiche Richtung gibt es aber sowohl in anderen Bundesländern als auch im Bund. So enthalten die Datenschutzgesetze der Länder Brandenburg[3], Bremen[4], Mecklenburg-Vorpommern[5] und Nordrhein-Westfalen[6] ebenfalls Bestimmungen über ein Datenschutzaudit oder auch Vorschriften über den vorrangigen Einsatz zertifizierter Produkte. In diesen Ländern fehlt es nur noch an entsprechenden Ausführungsbestimmungen, um diese gesetzlichen Ankündigungen in die Praxis umzusetzen.

Auch das Bundesdatenschutzgesetz (BDSG) enthält seit seiner Novellierung im Jahr 2001 in § 9a eine Ankündigung des Datenschutzaudits, dessen Ausgestaltung eines weiteren Gesetzes bedarf. Gemäß § 9a BDSG ist vorgesehen, dass Daten verarbeitende Stellen und Anbieter von Datenverarbeitungssystemen und -programmen ihr Datenschutzkonzept durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen können. Eine gleich lautende Regelung für ein Datenschutzaudit enthält ebenfalls das Sozialgesetzbuch X in § 78 c.

3.2 Geltung des schleswig-holsteinischen Gütesiegels in anderen Bundesländern

Nach dem LDSG SH sind schleswig-holsteinische Behörden unmittelbar verpflichtet, Produkte, die mit einem Datenschutz-Gütesiegel ausgezeichnet sind, vorrangig einzusetzen. Bei einer Beschaffung von IT-Produkten oder der Vergabe einer Auftragsdatenverarbeitung ist das Gütesiegel neben anderen Kriterien, wie etwa den Kosten, zu berücksichtigen. Sind zwei Produkte oder Dienstleistungen in allen Kriterien gleichwertig, aber nur eines davon mit einem Gütesiegel ausgezeichnet, so ist das zertifizierte Produkt zu bevorzugen.

Dieser direkte Wettbewerbsvorteil gilt unmittelbar jedoch nur für den Einsatz zertifizierter Produkte in Schleswig-Holstein. Da Hersteller oder Anbieter von Dienstleistungen in den meisten Fällen zumindest bundesweit agieren, stellt sich die Frage nach der Akzeptanz des schleswig-holsteinischen Gütesiegels außerhalb des Landes. Regelungen, die der Grundlage des schleswig-holsteinischen Gütesiegels ähnlich sind oder sogar entsprechen, enthalten wie bereits ausgeführt, mehrere Landesdatenschutzgesetze sowie das BDSG und das SGB X. Somit stellt sich die Frage, ob das Gütesiegel nach dem LDSG SH auch als ein Zertifikat nach diesen anderen Auditregelungen anerkannt werden kann. Für sämtliche dieser Auditregelungen fehlen bislang praktische Ausführungsregelungen, so dass es noch keine Zertifikate gibt, die mit dem schleswig-holsteinischen Gütesiegel in direkter Konkurrenz stehen und eine unmittelbare Frage nach der Gleichwertigkeit der Zertifikate hervorrufen.

Wenngleich wegen der unterschiedlichen Gesetzgebungskompetenzen der einzelnen Landesgesetzgeber und des Bundesgesetzgebers eine unmittelbare und automatische Geltung des schleswig-holsteinischen Gütesiegels nach den Vorschriften anderer Landes- oder Bundesgesetze wohl in den meisten Fällen nicht in Betracht kommt[7], so überschneiden sich die einzelnen Regelungen zum Datenschutzaudit inhaltlich jedoch beträchtlich. In der Praxis werden die Anforderungen an eine Zertifizierung nach dem LDSG SH den Anforderungen einer Zertifizierung nach anderen Gesetzen häufig weitgehend entsprechen. Eine vollständige Übereinstimmung der Anforderungen ist in solchen Fällen gegeben, in denen sich das datenschutzrechtliche Anforderungsprofil an das zu zertifizierende Produkt auf Grund seines Einsatzbereichs aus bundesrechtlichen Vorschriften ergibt, was im Medizinbereich häufig der Fall sein wird. Die rechtlichen Grundlagen in diesem Bereich entstammen zu einem wesentlichen Teil dem Bundesrecht (z.B. § 203 StGB, dem BDSG oder dem SGB). In solchen Fällen dürfte eine Anerkennung

und Berücksichtigung des schleswig-holsteinischen Gütesiegels auch nach anderen Auditregelungen leicht herbeizuführen sein. In der Praxis wird dies auch bereits vielfach entsprechend gehandhabt.

4 Anforderungen an Verfahren und Produkte im Medizinbereich

Die Anforderungen an Datenschutz und Datensicherheit im Bereich der Medizin ergeben sich aus den grundlegenden gesetzlichen Regelungen, die im Medizinbereich neben dem allgemeinen Datenschutzrecht (BDSG, Landesdatenschutzgesetze) der ärztlichen Schweigepflicht des § 203 Strafgesetzbuch und dem ärztlichen Standesrecht der Berufsordnungen für Ärzte entstammen.

Diese Vorschriften bilden die Grundlage sowohl für ein Auditverfahren als auch für die Zertifizierung von Produkten aus dem Medizinbereich. Für das Zertifizierungsverfahren sind in den Ausführungsregelungen des ULD weitere Besonderheiten geregelt, so dass im Folgenden im Wesentlichen das Verfahren zur Zertifizierung von Produkten betrachtet wird.

4.1 Prüfkriterien des ULD für die Produktzertifizierung

Unter welchen Voraussetzungen für ein IT-Produkt ein Gütesiegel erteilt werden kann, ergibt sich aus § 4 Abs. 2 LDSG in Verbindung mit § 2 Abs. 2 DSAVO. Danach muss das Produkt mit den Vorschriften über Datenschutz und Datensicherheit vereinbar sein und dabei insbesondere im Hinblick auf die folgenden Punkte besondere Eigenschaften aufweisen:

- Datenvermeidung und Datensparsamkeit
- Rechtmäßigkeit der Datenverarbeitung
- Datensicherheit und Revisionsfähigkeit der Datenverarbeitung
- Gewährleistung der Rechte der Betroffenen

Um die für das jeweilig betrachtete Produkt einschlägigen konkreten Anforderungen im Hinblick auf Datenschutz und Datensicherheit zu ermitteln, ist als Ausgangspunkt der für die Anwendung des Produkts vorgesehene Zweck und Einsatzbereich zu ermitteln und heranzuziehen. Bewegt sich das Produkt im Medizinbereich, so sind die oben genannten drei Bereiche (Datenschutzrecht, Schweigepflicht, Standesrecht) schnell als die einschlägigen Rechtsnormen ausgemacht. Anschließend ist weiter zu differenzieren, etwa danach ob das Produkt im öffentlichen oder im privaten Bereich angewendet werden soll (je nach dem kann entweder das BDSG oder das jeweils anwendbare Landesdatenschutzrecht zur Anwendung kommen) oder ob weitere spezielle Bereiche betroffen sind, für die es wiederum spezielle gesetzliche Regelungen gibt. Aus den ermittelten Rechtsvorschriften ergibt sich das rechtliche Anforderungsprofil, das der Begutachtung als Maßstab zu Grunde gelegt wird.

Zur Systematisierung und Konkretisierung der Anforderungen an das Produkt hat das ULD einen Anforderungskatalog erstellt, der die allgemeinen rechtlichen Anforderungen darstellt und diese um Fragen der technischen Umsetzung ergänzt. Der Anforderungskatalog gibt damit eine Mustergliederung für das Abarbeiten von Anforderungen und deren mögliche technische und organisatorische Umsetzung vor.

Entscheidend für die Vereinbarkeit des Produkts mit den so ermittelten Anforderungen ist die Umsetzung dieser Anforderungen durch das Produkt. Dabei ist grundsätzlich einer Umsetzung durch eine rein technische Lösung der Vorzug zu geben. Diese bietet den Vorteil, dass die Einhaltung der rechtlichen Forderungen automatisch sichergestellt und eine Umgehung – sei es aus Vorsatz oder aus Fahrlässigkeit – nicht möglich ist. Wo eine solche technische Lösung nicht realisierbar ist, können auch organisatorische Maßnahmen die Umsetzung der Anforderungen gewährleisten. Es ist dann aber erforderlich, dass die Produktbeschreibung diese organisatorischen Maßnahmen genau benennt und den Nutzer über die datenschutzgerechte Anwendung des Produkts umfassend aufklärt.

Der Produktbeschreibung kommt bei der Begutachtung und Zertifizierung des Produkts eine wesentliche Bedeutung zu. Sie hat die Funktion eines „Beipackzettels“, der den Nutzer über das Produkt, seine Konfiguration, die Datenschutz gerechte Anwendungsweise und Einsatzbedingungen sowie über Risiken – wenn möglich mit Hinweisen zur Abhilfe – informiert. Nur durch eine solche umfassende Information kann gewährleistet werden, dass ein Produkt, das in aller Regel auf vielfältige Art und Weise einsetzbar ist, Datenschutz gerecht angewendet wird. Aufgrund dieser grundlegenden Bedeutung wird die Produktbeschreibung als Teil des Produkts selbst angesehen und unterliegt ebenso der Prüfung und Begutachtung im Gütesiegelverfahren.

4.2 Technische Datenschutzanforderungen an die Telemedizin – Fallbeispiele

Durch Gestaltung von Technik gilt es, die Anforderungen der Rechtsvorschriften umzusetzen. Viele dieser teilweise restriktiven Regelungen lassen sich durch geeignete technische Lösungen in die Praxis umsetzen. So kann mit Hilfe differenzierter elektronischer Zugriffsverwaltung, dem Einsatz von digitalen Signaturen und Verschlüsselungstechniken und einer automatischen Protokollierung eine funktionsfähige medizinische Infrastruktur etabliert werden, die den hohen Anforderungen des Datenschutz- und Standesrechts genügt. Durch die Zuverlässigkeit technischer Systeme gegenüber der häufig fehleranfälligen menschlichen Tätigkeit kann sogar ein Mehr an Datenschutz gegenüber der konventionellen Datenverarbeitung erreicht werden. Einzelne medizinische Projekt können etwa durch die im Folgenden aufgeführten technischen Maßnahmen Datenschutz gerecht in die Praxis umgesetzt werden.

Zentrale digitale Patientendatenarchive können dadurch realisiert werden, dass durch den verantwortlichen Arzt eine Verschlüsselung erfolgt, die vom Archiv nicht aufgehoben werden kann. Dadurch können fast sämtliche technischen Verarbeitungprozesse an Dritte delegiert werden, ohne dass der Arzt seine Verantwortung für seine Daten aufgeben müsste. Voraussetzung ist nur, dass dem Archiv der Schlüssel nicht bekannt wird. So ist es auch möglich, von einer Vielzahl unterschiedlicher Ärzte und Einrichtungen Daten auf einem zentralen System verarbeiten zu können.

Datenschutz gerecht lässt sich auch ein Abruf von elektronisch gespeicherten

Daten durch Dritte realisieren. Hier muss vor jeder Abfrage eine Freischaltung durch den behandelnden Arzt erfolgen. Erfolgt dagegen der Abruf der Daten durch ein automatisiertes Abrufverfahren ohne Prüfmechanismus, entspricht dies nicht den Anforderungen des Datenschutzes. In einem solchen Fall würde bereits mit der Bereitstellung zum Abruf eine unbefugte Offenbarung erfolgen. Datenschutzfreundlich sind im Interesse der Patientenorientierung und im Hinblick auf das weitgehende Erfordernis der Patienteneinwilligung bei der Datenübermittlung dagegen insbesondere solche Verfahren, bei denen neben der ärztlichen Freischaltung auch eine technische Autorisierung durch die Patienten vorgesehen ist.

Die Authentifizierung des Arztes lässt sich mithilfe einer digitalen Signatur nachweisen. Hier bietet sich in überregionalen Netzen die Ärztechipkarte (Health Professional Card – HPC) an, die derzeit kurz vor der Markteinführung steht. Doch genügt eine solche Chipkarte allein nicht zum Nachweis für die Berechtigung zum Empfang medizinischer Daten im Einzelfall, wenn nicht die verantwortliche Stelle den Zugriff autorisiert hat. In überschaubaren Netzwerken kommen bei entsprechender Registrierung der Berechtigungen auch einfachere Authentifizierungsverfahren in Betracht, die mit persönlichen Identifikationen (Chipkartenbesitz, PIN, Biometrie), Rechneridentifikationen oder Programm-IDs arbeiten. Voraussetzung für die Zertifizierungsfähigkeit eines Zugriffsverfahrens sind beim Einsatz solcher Methoden aber zumindest doppelte Berechtigungskontrollen.

Die vollständige Übertragung der Datenhoheit auf den Patienten ist im Rahmen verbindlicher medizinischer Dokumentation nicht möglich. Im Interesse der Integrität und Authentizität medizinischer Daten muss regelmäßig ausgeschlossen sein, dass der Patient die gespeicherten Daten selbst verändern kann. Ebenso wird mit der Übertragung der Datenhoheit auf den Betroffenen – z. B. durch Speicherung auf einer Chipkarte oder durch unbegrenzte Zulassung eines Online-Abrufs – die Beschlagnahmesicherheit der Daten, die an die Datenhoheit des Arztes gebunden ist, aufgehoben. Es kann weiterhin das Risiko erhöht werden, dass Interessierte, z. B. Arbeitgeber oder Versicherungen, durch Druck auf den Patienten von diesem sensibelste Daten erlangen.

Von besonderer Bedeutung ist aufgrund der Sensibilität medizinischer Daten die Gewährleistung der Datensicherheit. An diese sind im Medizinbereich besonders hohe Anforderungen zu stellen. So ist z. B. der Zugriff zu elektronischen Datenbeständen durch andere als den behandelnden Arzt lückenlos für Kontrollzwecke zu protokollieren. Sollen Patientendaten über allgemein zugängliche offene Netze, z. B. über das Internet, übermittelt werden, kann dies nur zugelassen werden, wenn der Zugriff für Unbefugte durch eine ausreichende Verschlüsselung ausgeschlossen ist. Für die sichere Arzt interne Kommunikation ist die Nutzung eines abgeschotteten VPN (Virtual Private Network) naheliegend.

Weitere Informationen des Unabhängigen Landeszentrums für Datenschutz zum Gütesiegel unter www.datenschutzzentrum.de/guetesiegel, zum Datenschutzaudit unter www.datenschutzzentrum.de/audit und zum Thema Datenschutz im Medizinbereich unter www.datenschutzzentrum.de/medizin.

Literatur:

- Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002
- Bäumler, Marktwirtschaftlicher Datenschutz, DuD 2002, 325 ff
- Bizer/Petri, Kompetenzrechtliche Fragen des Datenschutz-Audits, DuD 2001, 97 ff
- Diek, Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz, in Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, S. 157 ff
- Golembiewski, Das Datenschutzaudit in Schleswig-Holstein, in Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, S. 107 ff
- Hansen/Probst, Datenschutzgütesiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels, in Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, S. 163 ff
- Weichert, Datenschutz-Audit und -Gütesiegel im Medizinbereich, Medizinrecht 2003, S. 675-681

Fußnoten

1 Die Landesverordnung über ein Datenschutzaudit (Gütesiegel-Verordnung - DSAVO) vom 3. April 2001, GVOBl. Schl.-H. 4/2001, S. 51 zur Regelung des Gütesiegels und die Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG, Amtsblatt Schl.-H. 13/2001, S. 196 zur Regelung des Datenschutzaudits

2 § 2 der Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutz-Verordnung - DSVO) vom 2. April 2001, GVOBl. Schl.-H. 4/2001, S. 49

3 § 11b Abs. 2 Brandenburgisches Datenschutzgesetz

4 § 7b Bremisches Datenschutzgesetz

5 § 5 Abs. 2 Landesdatenschutzgesetz Mecklenburg-Vorpommern

6 § 4 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen

7 Die meisten anderen Auditgrundlagen sehen eine Ausgestaltung durch weitere Gesetze vor, die durch den jeweiligen Landesgesetzgeber bzw. den Bundesgesetzgeber erlassen werden sollen. Eine Ausnahme bildet hier die Regelung des § 11b Abs. 2 des brandenburgischen Datenschutzgesetzes. Diese erfordert lediglich eine Prüfung der Produkte in einem förmlichen Verfahren, ohne nähere Anforderungen hierzu festzulegen bzw. die Festlegung einem weiteren Landesgesetz zu überlassen. Hier kommt tatsächlich eine unmittelbare Geltung des schleswig-holsteinischen Gütesiegelverfahrens als ein solches förmliches Verfahren in Betracht.