Empfehlungen
zur Protokollierung in zentralen IT-Verfahren
der gesetzlichen Krankenversicherung

(Arbeitskreis Gesundheit und Soziales / Arbeitskreis Technik
der Datenschutzbeauftragten des Bundes und der Länder;
von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf der Sitzung am 17./18.3.2010 zustimmend zu rKentnis genommen)

Stand: 19.3.2010

1. Einleitung

Änderungen der rechtlichen Rahmenbedingen im Gesundheitswesen, die Erweiterung funktionaler Anforderungen, Zusammenschlüsse von Krankenkassen sowie die technische Entwicklung haben im Bereich der gesetzlichen Krankenversicherung (GKV) zu einer grundlegenden Überarbeitung bzw. Neuentwicklung der eingesetzten IT-Verfahren geführt.

Diese decken weite Bereiche der Geschäftsfelder der Krankenkassen ab, wie

- Mitgliederverwaltung
- Leistungswesen
- Firmenkundenverwaltung
- Beitragswesen
- Entgeltersatzleistungen
- Elektronischer Datenaustausch
- Vertragswesen
- Kundenbeziehungen
- Unternehmenssteuerung / Controlling

Angesichts der Komplexität derartiger Großverfahren mit ihrer hohen Zahl von Benutzern und Transaktionen, verteilten IT-Strukturen und Verantwortlichkeiten bedarf es für eine datenschutzgerechte Gestaltung eines geeigneten Instrumentariums, um die Nutzung der Verfahren hinsichtlich der Verarbeitung personenbezogener Daten nachvollziehen zu können. Angesichts der Sensibilität der verarbeiteten Gesundheits- und Sozialdaten kommt dem besondere Bedeutung zu. Grundlage einer angemessenen Nachvollziehbarkeit ist eine aussagefähige Protokollierung einschließlich geeigneter Auswertungsmöglichkeiten.

Allgemeine Empfehlungen der Datenschutzbeauftragten zur Protokollierung in informationstechnischen Systemen ergeben sich aus der Orientierungshilfe "Protokollierung" des

Arbeitskreises Technik vom 2.11.2009
(http://www.datenschutz.rlp.de/downloads/oh/ak_oh_protokollierung.pdf); auf diese wird insoweit verwiesen. Die im Folgenden dargestellten Anforderungen orientieren sich in erster Linie an den Gegebenheiten bei zentralen Branchenanwendungen der Gesetzlichen Krankenversicherung. Sie behandeln lediglich die aus Datenschutzsicht relevanten Aspekte; Protokollierungen, die im Rahmen des rein technischen Verfahrensbetriebs erfolgen, werden nicht betrachtet.

2. Rechtliche Grundlagen

Soweit nicht bereichspezifische Rechtsgrundlagen im Bereich der GKV Vorgaben hinsichtlich der Nachvollziehbarkeit formulieren (z.B. § 276 Abs. 2, § 291a Abs. 5 und 6 SGB V, § 79 Abs. 4 SGB X) gründen die entsprechenden Anforderungen auf § 78a SGB X. Danach sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Sozialgesetzbuchs zu gewährleisten. Die Notwendigkeit einer Protokollierung ergibt sich dabei aus Nr. 4 und 5 der Anlage zu § 78 a SGB X sowie – als vorbeugende Maßnahme der Zugangs- und Zugriffskontrolle - aus Nr. 2 und 3.

Des Weiteren hat der Europäische Gerichtshof für Menschenrechte in einem Urteil aus dem Jahr 2008 (ECHR Application No. 20511/03) im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems entschieden, dass in der fehlenden Protokollierung von (lesenden) Zugriffen auf medizinische Daten ein Verstoß gegen Artikel 8 der Europäischen Menschenrechtskonvention liegt.

3. Art und Umfang der Protokollierung sowie deren Nutzung

Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten insoweit transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat. Ihre Nutzung für Revisions- und Beweiszwecke erfordert, dass sie vollständig und nur den zur Nutzung Berechtigten zugänglich sind und nicht nachträglich verändert werden können. Zur Wahrung der Vertraulichkeit, Integrität und Authentizität sind geeignete kryptografische Verfahren nach dem Stand der Technik einzusetzen.

Auch für die Gestaltung von Protokollierungsverfahren gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken (siehe hierzu Tz. 3.1 bis 3.3).

Aufgrund bestehender Revisionsanforderungen bzw. des Unternehmensinteresses an einer integren und konsistenten Datenbasis ist in IT-Verfahren häufig bereits eine Protokollierung schreibender bzw. ändernder Zugriffe vorgesehen. Dies entspricht der Eingabekontrolle nach Nr. 5 der Anlage zu § 78a SGB X. Da die datenschutzrechtliche Bewertung nach § 78a

SGB X insbesondere auch die Frage der zulässigen Kenntnisnahme personenbezogener Daten betrifft, bedarf es darüber hinaus einer Protokollierung auch lesender Zugriffe. Erkenntnisse aus der Kontrollpraxis der Datenschutzbeauftragten zeigen, dass trotz entgegenstehender Regelungen in Informationssystemen bestehende Recherche- und Auswertungsmöglichkeiten auch für Abfragen genutzt werden, bei denen das Vorliegen eines sachlichen Grundes zweifelhaft ist. Neben einem stringenten Berechtigungskonzept kann dem nur mit einer Protokollierung lesender Zugriffe begegnet werden. Einem oftmals nur geringen Entdeckungsrisiko missbräuchlicher Zugriffe müssen geeignete Aufklärungsmöglichkeiten – auch mit Blick auf deren präventive Wirkung – gegenüberstehen.

Die Protokollierung von Zugriffen, schreibender als auch lesender, bzw. die Protokollierung von Abfragen und Auswertungen ist bei entsprechender Gestaltung auch in Großverfahren grundsätzlich technisch umsetzbar und praktikabel. Der konzeptionelle Aufwand hierfür ist überschaubar, insbesondere dann, wenn dies bereits bei der Verfahrenskonzeption berücksichtigt wird.

Eine Protokollierung lesender Zugriffe ist aus Gründen der datenschutzrechtlichen Revisionssicherheit grundsätzlich erforderlich. Es sind Mechanismen zu schaffen, mit denen lesende Zugriffe orientiert an der Kategorie der Daten bzw. der genutzten Funktionen differenziert protokolliert werden können. Der Umfang der Protokollierung korrespondiert dabei mit den bestehenden Zugriffsregelungen. Bei hinreichend fein differenziertem Zugriffsschutz kann eine Protokollierung reduziert werden; umgekehrt steigt ihre Bedeutung in den Bereichen mit weit gefassten (Abfrage-) Berechtigungen.

Die Protokollierung sollte möglichst auf Transaktionsebene erfolgen, um eine an der fachlichen Verfahrenslogik bzw. den jeweiligen Geschäftsprozessen orientierte Nachvollziehbarkeit zu ermöglichen. Eine Protokollierung auf Datenbankebene oder eine technische Protokollierung ohne Bezug zum sachlichen Zusammenhang eines Zugriffs trägt dem nicht Rechnung. Ebenso genügt eine technisch mögliche Protokollierung lesender Zugriffe, die aufgrund daraus resultierender Datenvolumina und Leistungseinbußen letztlich nicht eingesetzt wird, den datenschutzrechtlichen Anforderungen nicht.

Hinsichtlich einer datenschutzrelevanten Protokollierung ist zwischen Zugriffen, die aus der fachlichen Nutzung des Verfahrens resultieren und administrativen Zugriffen im Rahmen des System- und Verfahrensbetriebs zu differenzieren.

3.1 Protokollierung von Daten aus der Verfahrensnutzung

Bei der Nutzung von Verfahren zur automatisierten Verarbeitung personenbezogener Daten ist die Protokollierung zum Nachweis einer korrekten, rechtskonformen Verarbeitung geboten. Die Inhalte der Protokolldaten orientieren sich hierbei an der Art der Verarbeitung und am Schutzbedarf der jeweiligen Daten. Damit ist es nicht zwingend erforderlich, jeglichen Zugriff zu protokollieren. Im Interesse einer sinnvollen Begrenzung und Auswertbarkeit - und unter Berücksichtigung bestehender Zugriffsbeschränkungen - kann es ange-

bracht sein, die Protokollierung vorrangig auf Zugriffe in bestimmten Bereichen auszurichten.

Dies sind im Bereich der GKV insbesondere Aufrufe von Transaktionen und Reports zu

- Stammdaten von Versicherten/Kunden,
- Fall- und Leistungsübersichten,
- versichertenbezogenen Gesundheitsdaten,
- versichertenbezogenen Leistungsdaten,
- Verordnungen und Belegen,
- medizinischen Daten,
- ärztlichen Berichten,
- Gutachten,
- Datensätzen besonderer Personengruppen (z.B. Mitarbeiterdaten, VIPs)
- Daten außerhalb des fachlichen oder regionalen Zuständigkeitsbereichs des Benutzers,
- gesperrten Fällen sowie die
- Rückweisungen aufgrund fehlender Berechtigungen.

Ob auf eine Protokollierung in den genannten Bereichen ganz oder teilweise verzichtet werden kann, hängt im Einzelfall von den sachlich oder regional beschränkten Zugriffsmöglichkeiten der Nutzer ab. Des Weiteren kann eine Protokollierung entbehrlich sein, wenn Zugriffe im Rahmen technisch festgeleger Geschäftsprozesse erfolgen, bei denen in wiederkehrender Weise bestimmte Verarbeitungsschritte aufeinanderfolgen (Workflow) und dies anhand einer Fachdokumentation nachvollziehbar ist (z.B. automatisch gesteuerter Verarbeitungsprozess von der Beantragung eines Hilfsmittels bis zur Genehmigung / Bereitstellung). Der konkrete Umfang der Protokollierung sollte im Rahmen der Grundkonfiguration des Verfahrens mit dem internen Datenschutzbeauftragten abgestimmt werden.

Eine angemessene Nachvollziehbarkeit ist im Allgemeinen bei der Erfassung folgender Angaben sichergestellt:

- Authentifizierung und Autorisierung (Login/Logout),
- Zeitpunkt eines Zugriffs,
- Kennung des jeweiligen Benutzers,
- Kennung der jeweiligen Arbeitsstation,
- aufgerufene Transaktion (Anzeige-/Abfragefunktion, Reportname, Maskenbezeichnung),
- verwendete Such- bzw. Abfragekriterien (z.B. Versichertennummer, Name, Geburtsdatum, Wohnort, Fallnummer etc.),
- Ergebnis der Abfrage (z.B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske; i.d.R. jedoch keine Datensatzinhalte),
- etwaige Folgeaktionen bzw. Navigationsschritte (z.B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).

Die Löschung von Daten ist Teil einer Protokollierung ändernder Zugriffe und sollte lediglich insoweit erfasst werden, als für einzelne Daten der Zeitpunkt der Löschung und der jeweilige Benutzer, für Datensätze zusätzlich die jeweilige Versicherungs- bzw. Fallnummer oder vergleichbare Identifikationsmerkmale festgehalten werden.

3.2 Protokollierung administrativer Zugriffe

Das Administrationspersonal verfügt regelmäßig über Zugriffsrechte, die über das zur üblichen Verfahrensnutzung notwendige Maß hinausgehen. Beschränkungen, denen die fachlichen Nutzer eines Verfahrens unterliegen, gelten für die Administration in der Regel nicht. Die Wahrnehmung administrativer Funktionen bedarf damit einer besonderen Kontrolle. Dabei ist auch zu sehen, dass die Protokollierung außer für datenschutzrechtliche Zwecke auch zum Schutz der Administration vor unberechtigten Vorwürfen hinsichtlich missbräuchlicher Zugriffe dienen kann. Ohne eine entsprechende Protokollierung könnten solche Vorwürfe gegen Administratoren nicht nachhaltig entkräftet werden.

In diesen Bereich der Protokollierung fallen alle Zugriffe im Rahmen der technischen und fachlichen Verfahrensbetreuung, die Auswirkungen auf Art oder Umfang der Verarbeitung personenbezogener Daten haben, insbesondere:

- Maßnahmen der Installation / Deinstallation von Software,
- Änderungen der Anwendungskonfiguration (z.B. Customizing, Festlegen von Migrationsregeln, Residenzzeiten / Löschfristen, Login-Parameter, Anzeigeparameter, usw.),
- Zugriffe im Rahmen einer etwaigen Mandantenverwaltung,
- die Anlage, Änderung und Löschung von Rollen,
- die Vergabe, Änderung und Löschung von Berechtigungen,
- die Administration von Benutzern (Anlage, Sperre, Löschung, Rollenzuweisung),
- die Einrichtung / Änderung standardmäßig vorgegebener Auswertungsmöglichkeiten (Reports),
- der Import / Export von Datenbeständen,
- Datenübermittlungen,
- Prozesse zur Aggregierung, Pseudonymisierung / Anonymisierung von Datenbeständen (Date Warehouse),
- Archivierungen / Datensicherungen.

Vergleichbar der Aufteilung administrativer Funktionen auf eine Verfahrens- und eine Benutzer- bzw. Berechtigungsadministration dürfen Zugriffe auf die zur Datenschutzkontrolle erzeugten Protokolldaten nicht dem Personenkreis möglich sein, dessen Zugriffe gerade über die Protokollierung dokumentiert werden. Im Rahmen einer angemessenen Zugriffskontrolle für die Protokolldaten sollten daher kryptografische Verfahren zum Einsatz kommen oder ein Zugriff nur nach dem 4-Augen-Prinzip (Administration / Datenschutzbeauftragter) möglich sein.

3.3 Umfang der Protokollierung

Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien

Im Gegensatz zur Protokollierung schreibender Zugriffe, bei der in der Regel der Zustand vor und nach der jeweiligen Änderung erfasst wird, ist bei lesenden Zugriffen die Speicherung des Inhalts der betroffenen Datensätze weitgehend entbehrlich. Dies gilt insbesondere dann, wenn bei Bedarf der Inhalt eines Datensatzes zum Zeitpunkt des Zugriffs über eine vorhandene Protokollierung der Datenspeicherung und -änderung festgestellt werden kann. Im Übrigen handelt es sich um Daten, die nicht zwingend im unmittelbaren Zugriff stehen müssen, so dass über ein Archivierungskonzept eine frühzeitige Auslagerung der Protokolldaten vorgesehen werden kann.

Angesichts der Nutzungsszenarien bei GKV-Verfahren besteht eine angemessene Nachvollziehbarkeit nur auf der Grundlage einer vollständigen Erfassung der nach Tz. 3.1 und 3.2 als protokollrelevant deklarierten Zugriffe. Eine stichprobenweise Protokollierung oder die Protokollierung lediglich eines bestimmten Anteils von Zugriffen hat sich für eine effektive Datenschutzkontrolle als untauglich erwiesen, da bei anlassbezogenen Auswertungen relevante Zugriffe im Zweifelsfall nicht oder nur unvollständig erfasst sind.

Art und der Umfang der Protokollierung sind im Rahmen der Verfahrensentwicklung in einem Protokollierungskonzept zu dokumentieren.

4. Zweckbindung

Protokolldaten unterliegen einer strikten, in den Datenschutzgesetzen von Bund und Ländern geregelten Zweckbindung (z. B. § 31 BDSG, § 13 Abs. 6 LDSG Rheinland-Pfalz).

Sie dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die nach datenschutzrechtlichen Vorschriften geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden (z. B. § 81 Abs. 4 SGB X i.V.m. § 4g Abs. 1 und § 18 Abs. 2 BDSG) und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z. B. zur Strafverfolgung, zu.

Protokolldaten dürfen nicht für eine automatisierte allgemeine Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden. Eine stichprobenweise oder anlassbezogene Auswertung von Protokolldaten im Rahmen der Datenschutzkontrolle ist keine derartige allgemeine Verhaltens- und Leistungskontrolle. Sie ist ebenfalls keine Vorratsdatenspeicherung; letztere erfolgt zu unbestimmten Zwecken, ein solcher (Datenschutzkontrolle) ergibt sich für die Protokolldaten jedoch aus § 31 BDSG.

Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden (vgl. Tz. 3.1).

5. Nutzung von Protokolldaten, Auswertung

Bei Protokolldaten handelt es sich um personenbezogene Daten, die, je nach Umfang, einen umfassenden Einblick in die Tätigkeiten der Administratoren, und Nutzer bzw. Anwender ermöglichen. Sie unterliegen bei ihrer Speicherung und weiteren Verarbeitung bzw. Nutzung ihrerseits datenschutzrechtlichen Vorschriften. Im Rahmen der Zugriffskontrolle ist damit zu gewährleisten, dass eine Einsichtnahme nur den Personen möglich ist, in deren Aufgabenbereich etwaige Auswertungen fallen.

Auswertungen dürfen entsprechend der unter Tz. 4 genannten Zweckbindung grundsätzlich nur zur Datenschutzkontrolle erfolgen. Hierunter fällt in erster Linie die Klärung sich im Einzelfall ergebender Fragen, denen ein konkreter Anlass wie z.B. eine Eingabe oder ein Auskunftsersuchen eines Betroffenen, der Verdacht auf einen missbräuchlichen Datenzugriff oder eine Kontrollmaßnahme der Datenschutzaufsichtsbehörde zugrunde liegt. Der jeweilige Anlass ist nachvollziehbar zu dokumentieren. Daneben können, fallweise oder regelmäßig, zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme anlassunabhängige Auswertungen vorgenommen werden (vgl. § 81 Abs. 4 SGB X i.V.m. § 4g Abs. 1 Nr. 1 BDSG). Im Rahmen einer vorbeugenden Datenschutzkontrolle kommt es weiterhin in Betracht, die Protokolle turnusmäßig auf bestimmte Auffälligkeiten hin, wie auffällige Häufungen von Abfragen bestimmter Benutzerkennungen, eine Häufung von Abfragen außerhalb der Bürozeiten, unübliche Suchkriterien oder kritische Transaktionen hin auszuwerten. Der mit der Auswertung verfolgte Zweck und deren Ergebnis sind zu dokumentieren.

Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten entsprechend der unter Tz. 3 dargestellten Gesichtspunkte auswerten zu können. Dies erfordert eine Auswertbarkeit z.B. nach Benutzerkennungen, Arbeitsstationen, Funktionen / Transaktionen, Versichertennummern/Fallnummern, Zeiträumen oder Suchkriterien. Hierzu sollten bereits im Verfahren selbst Auswertungsmöglichkeiten vorgesehen werden, die eine schnelle Selektion prüfungsrelevanter Datensätze erlauben.

Struktur und Format der Protokolldaten müssen es ermöglichen, dass bei Bedarf auch eine flexible Auswertung der Protokolle erfolgen kann. Die Protokolldaten müssen daher in einem durch gängige Analysewerkzeuge oder Datenbnakfunktionen auswertbaren Format vorliegen bzw. in ein solches überführt werden können (z.B. CSV-Format mit geeigneten Trennzeichen, je Protokolleintrag eine Zeile). Im Interesse der zeitlichen Eingrenzbarkeit und der leichteren Steuerung von Aufbewahrungsfristen sollte möglichst eine tages- oder monatsbezogene Speicherung erfolgen.

Abhängig von den zugrundeliegenden rechtlichen Vorgaben setzt die Einführung eines Protokollierungsverfahrens u.U. die Mitbestimmung durch die Personalvertretung voraus. Aus datenschutzrechtlicher Sicht sollte auf jeden Fall für die Auswertung von Protokolldaten unter Berücksichtigung der vorstehend genannten Punkte und Festlegung der Beteiligten eine Verfahrensweise bestimmt werden.

6. Speicherungsdauer

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die Erforderlichkeit zur Aufgabenerfüllung einschließlich der Erfordernisse einer ordnungsgemäßen Dokumentation. Als Anhaltspunkte dienen die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und die Notwendigkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle aufklären zu können. Im Allgemeinen ist danach eine Aufbewahrungsdauer von zwölf Monaten als ausreichend anzusehen.

Anderes gilt für die Daten aus der Protokollierung administrativer Zugriffe, insbesondere , soweit sie Konfigurationsänderungen und Datenübermittlungen betreffen. Diese sind als Teil der Verfahrensdokumentation anzusehen, da sie nicht in erster Linie die Nutzung eines Verfahrens dokumentieren, sondern dessen Betrieb. Hier sind längere Aufbewahrungsfristen, orientiert an der Dauer des Einsatzes eines Verfahrens vorzusehen.

Soweit Protokolle eigens zum Zweck gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsfrist vorzusehen; in der Regel reicht hier eine Aufbewahrung bis zum Abschluss der Kontrolle aus. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (vgl. § 20 Abs. 2 BDSG).

Die vorstehend genannten Punkte sind für das jeweilige GKV-Verfahren in einem Protokollierungskonzept zusammenzufassen, das Art und Umfang der Protokollierung, die Verfahrensweisen zur Speicherung und Auswertung der Protokolldaten sowie die in diesem Zusammenhang getroffenen Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen beschreibt.