

Sehr geehrter Herr Dolle,

der Arbeitskreis "Gesundheit und Soziales" der Datenschutzbeauftragten des Bundes und der Länder nimmt - wegen der besonderen Bedeutung des Aktionsforums Telematik im Gesundheitswesen (ATG) für die Entwicklung der Telematik in Deutschland - zusätzlich zu den Stellungnahmen des Hessischen Landesbeauftragten für den Datenschutz vom August 2000 und des Bayerischen Landesbeauftragten für den Datenschutz vom 07. August 2000 zum Managementpapier des ATG zum elektronischen Arztbrief, das der Arbeitskreis insgesamt als einen aus datenschutzrechtlicher Sicht positiven Ansatz zur praktischen Umsetzung dieser telemedizinischen Anwendung ansieht, im einzelnen wie folgt Stellung:

Zentraler Gesichtspunkt aus datenschutzrechtlicher Sicht muss bei der Anwendung der Telemedizin sein, dass die bestehenden Patientenrechte auch unter den Bedingungen moderner Technik gewahrt bleiben. Der Schutz der Patientendaten darf sich durch die Telemedizin nicht verschlechtern, wünschenswert wäre eine nachhaltige Verbesserung. Die Kommunikationsprozesse müssen unter Beachtung der datenschutzrechtlichen und der sicherheitstechnischen Rahmenbedingungen ausgestaltet werden.

Der Arbeitskreis weist daher auf folgende grundsätzliche datenschutzrechtliche Anforderungen hin:

* Auch bei der telemedizinischen Anwendung elektronischer Arztbrief ist die in den Berufsordnungen für die Ärzte und Ärztinnen enthaltene ärztliche Schweigepflicht, die in § 203 Abs. 1 Satz 1 StGB strafbewehrt ist, zu beachten. Für Datenverarbeitungen in der Telemedizin, insbesondere für die Übermittlung personenbezogener Patientendaten, muss - wie in der "traditionellen" Medizin - eine Offenbarungspflicht oder eine Offenbarungsbefugnis vorliegen. Dabei sind ggf. der Behandlungsvertrag, die ärztlichen Berufsordnungen, die (freiwillige und informierte) Einwilligung der Patienten, sowie die bereichsspezifischen (z. B. Krankenhausgesetze) und die allgemeinen Datenschutzgesetze (BDSG und Landesdatenschutzgesetze) zu beachten. Je nach Anwendungsbereich ist die ärztliche Kommunikation ggf. auch in den einzelnen Büchern des Sozialgesetzbuches (SGB) geregelt, vgl. etwa § 73 Abs. 1b SGB V (Hausarztmodell) und § 140a Abs. 2 SGB V (Integrierte Versorgung).

* Ferner müssen die bestehenden Patientenrechte gewahrt bleiben (z. B. Rechte auf Benachrichtigung, Auskunft, Einsicht, Berichtigung, Löschung oder Sperrung der Daten). Diese Rechte sind durch eine effektive Gestaltung der Verfahren sicher zu stellen.

* Selbst bei Vorliegen einer Rechtsgrundlage für die personenbezogene bzw. personenbeziehbare Offenbarung von Patientendaten ist zu fragen, ob nicht die Verarbeitung anonymisierter oder pseudonymisierter Daten (z. B. bei Qualitätssicherungsverfahren) für die Erreichung des beabsichtigten Zwecks ausreicht (Grundsatz der Erforderlichkeit).

- * Falls keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorliegt, ist in der Regel - auch für die Verarbeitung personenbezogener Daten mittels eines elektronischen Arztbriefs - die freiwillige, informierte und grundsätzlich schriftliche Einwilligung der Patienten erforderlich. Eine mutmaßliche Einwilligung kann nur in Ausnahmefällen (z. B. Notfälle) angenommen werden, wenn die Datenverarbeitung im vermeintlichen Interesse und Einverständnis des Patienten erfolgt und eine ausdrückliche Einwilligung nicht rechtzeitig eingeholt werden kann.
- * Eine pauschale und vorab für alle (telemedizinischen) Behandlungen erklärte Einwilligung der Patienten in die künftige Verarbeitung medizinischer Daten, deren Umfang und Tragweite sie zum Zeitpunkt der Erklärung nicht übersehen können, erfüllt nicht die datenschutzrechtlichen Anforderungen an die Informiertheit der Einwilligung und ist nicht ausreichend.
- * Bei der technischen und organisatorischen Ausgestaltung der Verfahren müssen die grundlegenden Anforderungen der Datenschutzgesetze an technische und organisatorische Maßnahmen beachtet werden (vgl. z. B. die Anlage zu § 9 BDSG). Sicherungsmaßnahmen müssen vor allem die Verfügbarkeit, die Authentizität, die Integrität und die Vertraulichkeit der Daten gewährleisten. Die eindeutige Verantwortlichkeit für die Richtigkeit der Daten ist sicher zu stellen. Eine vertrauliche ärztliche Kommunikation muss - z. B. durch eine sichere Verschlüsselung - gewährleistet werden.
- * Da es sich bei (tele-)medizinischen Datenverarbeitungen um automatisierte Verarbeitungen sensibler personenbezogener Daten mit spezifischen Risiken für die Rechte und Freiheiten Betroffener handelt, verlangen Art. 20 Abs. 1 der EG-Datenschutzrichtlinie und § 4d Abs. 5 des BDSG-Entwurfs (Stand: 14.06.2000) die Durchführung einer Vorabkontrolle vor Beginn der Verarbeitung durch den internen Datenschutzbeauftragten. Im Rahmen dieser Vorabprüfung ist auch die datenschutzgerechte technisch-organisatorische Ausgestaltung des Verfahrens zu bewerten.

Mit freundlichen Grüßen

gez.
Reinhard Vetter

Geschäftsstelle des Bayer. Landesbeauftragten für den Datenschutz
Wagmüllerstraße 18 - 80538 München
Postfach 22 12 19 - 80502 München
Tel. +49 89 212672-0 Fax +49 89 212672 50