International Working Group
on Data Protection
in Telecommunications

675.32.29

Arbeitspapier zur Online-Verfügbarkeit elektronischer Gesundheitsdaten

- Übersetzung -

39. Sitzung, 6. – 7. April 2006
Washington D. C. (USA)

Die Arbeitsgruppe hat die steigende Bedeutung Web-basierter Telemedizin bereits in der Vergangenheit unterstrichen[1]. Die Verfügbarkeit elektronischer Gesundheitsdaten in Netzwerken (insbesondere im Internet) während der Lebenszeit eines Patienten und darüber hinaus wirft komplexe zusätzliche Fragen auf. Diese Online-Verfügbarkeit elektronischer Gesundheitsdaten wird hauptsächlich aus den folgenden Gründen favorisiert:

- geringere Kosten für die Verarbeitung medizinischer Daten,
- die unmittelbare, „ubiquitäre" und (scheinbar) komplette Verfügbarkeit der Daten
    - für Doktoren, um zur Gesundheit des Patienten beizutragen,
    - für die Patienten selbst,
- der Patient könnte seine oder ihre Einwilligung online leichter als offline geben.

Gesundheitsinformationen in Netzwerken könnten auch für Forschungs- und Qualitätsmanagementszwecke genutzt werden. Die Diskussion der weitergehenden Implikationen dieser Entwicklung kann in dieser Arbeitsgruppe nicht geführt werden. Es ist allerdings darauf hinzuweisen, dass elektronische Gesundheitsinformationen in Netzwerken generell das Interesse von Dritten auf sich ziehen werden, wie z. B. von Versicherungsunternehmen und Strafverfolgungsbehörden.

Die besondere Sensitivität von Gesundheitsdaten muss bedacht werden, wenn die Online-Verfügbarkeit elektronischer Gesundheitsdaten erwogen wird. Ärzte haben von je her die Verpflichtung gehabt, Informationen von Patienten unter dem hippokratischen Eid[2] sind vertraulich zu behandeln. Die Aufgabe, sich um die Gesundheit und das Leben des Patienten zu kümmern, war nie eine Rechtfertigung dafür, solche Informationen an Dritte weiterzugeben, die nicht an der Behandlung des einzelnen Patienten beteiligt sind.

---

[1] Arbeitspapier zu „netzwerkbasierte Telemedizin", angenommen auf der 31. Sitzung am 26./27. März 2002 in Auckland (Neuseeland) – aktualisiert auf der 38. Sitzung am 6./7. September 2005 (Berlin) <http://ww.datenschutz-berlin.de/attachments/208/wpmed_de.pdf>

[2] „Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und was man nicht nach außen tragen darf, werde ich schweigen und es geheim halten. Wenn ich diesen Eid erfülle und ihn nicht verletzte, so möge ich mein Leben und meine Kunst genießen, respektiert von allen Menschen für alle Zeiten. Wenn ich ihn aber übertrete oder ihn verletze, dann soll das Gegenteil davon mein Los sein."

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Heutzutage ist die Vertraulichkeit medizinischer Informationen in den meisten Ländern durch Strafgesetze geschützt. In einigen Ländern ist sogar die Beschlagnahme medizinischer Daten für Strafverfolgungszwecke verboten, soweit diese Daten im Besitz eines Arztes oder eines Krankenhauses sind. Dieser Standard muss auch aufrecht erhalten werden, wenn elektronische Gesundheitsdaten online gestellt werden sollen. Der Grad des Schutzes für Gesundheitsdaten des Patienten darf nicht davon abhängen, ob diese in konventioneller Weise in einer Akte gespeichert werden oder in einem Netzwerk.

Gesundheitsdaten zählen zu den sensitivsten und privatesten Informationen über den Einzelnen. Die Offenlegung eines Gesundheitszustandes oder einer Diagnose könnte das persönliche und berufliche Leben eines Einzelnen negativ beeinflussen. Sogar die Offenlegung einer geringfügigen Gesundheitsangelegenheit kann für den Patienten peinlich sein und ihn möglicherweise davon abhalten, in Zukunft professionelle medizinische Beratung in Anspruch zu nehmen. Beispiele für Diskriminierung infolge von nicht-authorisierter Weitergabe medizinischer Daten existieren auch bei traditioneller, papierener Aktenhaltung[3]. Betroffenen sind bereits die Einstellung in ein Arbeitsverhältnis, Versicherungen und Kreditzusagen wegen der Offenlegung medizinischer Informationen an unberechtigte Parteien verweigert worden. Die Aufbewahrung medizinischer Daten in elektronischer Form erhöht das Risiko, dass Patienteninformationen unbeabsichtigt offenbart oder in einfacher Weise an unberechtigte Parteien weitergegeben werden können.

Darüber hinaus gibt die Nutzung des unsicheren Internets und – sogar in noch größerem Maße – von ungeschützten drahtlosen Netzwerken[4] zur Speicherung und Übertragung von Gesundheitsdaten Anlass zu besonderen Besorgnissen.

Empfehlungen

Die Arbeitsgruppe gibt daher die folgenden vorläufigen Empfehlungen, die im Lichte zukünftiger rechtlicher Entwicklungen und technologischer Innovationen überprüft werden müssen:

1. Es muss sorgfältig evaluiert werden, welche Kategorien medizinischer Daten in elektronischer Form verfügbar gemacht oder online gestellt werden sollen. Bestimmte Kategorien von Gesundheitsdaten wie genetische oder psychiatrische Daten könnten von der Online-Verarbeitung insgesamt ausgeschlossen werden, oder zumindest besonders strikten Zugriffsbeschränkungen unterliegen müssen.

2. In jedem Fall sollte es der autonomen und freien Entscheidung des Patienten - unterstützt durch nutzerfreundliche Technologien - überlassen werden, welche personenbezogenen Gesundheitsdaten über ihn in einem elektronischen Gesundheitsdatensatz oder in einem Netzwerk gespeichert oder weitergegeben werden sollen, soweit dies nicht ausdrücklich durch nationales Gesetz verlangt wird. Diese Entscheidung soll die Möglichkeit der relevanten Gesundheitsdienste oder Ärzte, solche Informationen für Behandlungszwecke zu speichern, unberührt lassen. Die Einwilligung muss immer eine fundamentale Anforderung im medizinischen Bereich sein. Eine strikte Zweckbindung ist auch in einer online-Umgebung essentiell. Zu diesem Zweck müssen Gesundheitseinrichtungen ein internes Zugriffskontrollsystem implementieren, das ausreichend ist, die Privatsphäre des Patienten zu schützen.

3. Die Patienten müssen umfassend über die Art der Daten und die Struktur der elektronischen Gesundheitsdatensätze, in denen die Daten enthalten sind, informiert werden. Die Patienten sollten eine Alternative (konventionelle) Möglichkeit haben, über die auf sie bezogenen medizinischen Informationen Zugriff zu erhalten.

4. Es gibt zusätzliche Herausforderungen für die Vertraulichkeit, die der Online-Verfügbarkeit von Gesundheitsdaten inhärent ist. Die bloße Übertragung von gesetzlichen Standards zur Vertraulichkeit, die in einem traditionellen Umfeld mit papierenen Akten gelten, könnte unzureichend sein, um das Interesse eines Patienten an seiner Privatsphäre zu schützen, wenn elektronische Gesundheitsinformationen online verfügbar gemacht werden. Personenbezogene Gesundheitsinformationen dürfen nur in offenen Netzwerken verarbeitet werden, wenn diese durch starke Verschlüsselung und sichere Authentifizierungsmechanismen geschützt sind. Nur autorisiertem, medizinisch qualifiziertem Personal

[3] Siehe „Health Privacy Project, Medical Privacy True Stories (10. November 2003), unter http://www.patientprivacyrights.org/site/DocServer/True_Stories.pdf?docID=321.

[4] Vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen; verabschiedet am 15. April 2004 bei 35. Sitzung in Buenos Aires; http://www.datenschutz-berlin.de/attachments/196/1_de.pdf

sollte erlaubt werden, auf spezifische Teile der elektronischen Gesundheitsakte online zuzugreifen, soweit dies unbedingt notwendig ist, und Zugriffe sollten protokolliert werden. Die Daten müssen und richtig und aktuell gehalten werden. Patienten sollte eine nutzerfreundliche Möglichkeit haben, auf seine Protokolldaten online zuzugreifen, um in der Lage zu sein, festzustellen, wer auf seinen oder ihren Gesundheitsdatensatz zugegriffen hat.

5. Die Arbeitsgruppe empfiehlt die Entwicklung von Sicherheitsmindeststandards für den Umgang mit elektronischen Gesundheitsdaten. Diese sollten Standards zur Datenverschlüsselung enthalten, sowie Autorisierungsmechanismen, Transaktionsüberwachungsprozeduren, und Zugriffskontrollsysteme. Die Entwicklung von Grundschutzstandards würde betriebliche Datenschutzbeauftragte und Archivare von Daten in die Lage versetzen, den Patientendatenschutz sicherzustellen und gleichzeitig die Vorteile eines elektronischen Aktenhaltungssystems zu genießen. Die Arbeitsgruppe ermutigt alle Interessengruppen (öffentliche Einrichtungen, den Gesundheitssektor, die Industrie und Standardisierungsorganisationen) datenschutzkonforme Technologien für das elektronische Gesundheitswesen zu entwickeln und anzuwenden, die die notwendige Vertraulichkeit und Sicherheit bieten. Die Arbeitsgruppe begrüßt die gegenwärtig in der Internationalen Organisation für Standardisierung (ISO) diskutierte Initiative zur Verabschiedung eines Sicherheitsstandards für den Medizin- und Gesundheitssektor (mit dem Entwurf des ISO-Standards 27799, der den Informationssicherheits-Management ISO-Standard 17799 für den Gesundheitssektor adaptiert). Es muss jedoch festgestellt werden, dass diese internationalen Standards nationale Gesetzgebung zum Datenschutz nicht ersetzen können.

Die Arbeitsgruppe lädt den medizinischen Berufsstand und die Öffentlichkeit dazu ein, diese Empfehlungen zu kommentieren.