Newsletter Datenschutz Ausgabe 2 | Mai 2012

DaSuMed

Datenschutzinfos für medizinische und soziale

Liebe Kolleginnen und Kollegen,

mit diesem Newsletter erreichen Sie die neuesten datenschutzrechtlichen Informationen der letzten Wochen mit Bezügen zu medizinischen und sozialen Einrichtungen.

Mit besten Grüßen, Mark Rüdlin

1. In den Startlöchern stehende neue EU-Datenschutzverordnung

Im Januar 2012 stellte die EU-Kommission den Entwurf der neuen EU-Datenschutzverordnung (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF) vor. Viele Änderungen und Neuerungen finden sich dort, z. B. das „Recht auf Vergessen werden“ und ein verstärkter Schutz von Kindern. Eine Änderung mit gravierenden Auswirkungen sollte schon einmal in den Blick genommen werden: Vorabkontrolle und Erstellung von Verfahrensverzeichnissen fallen zukünftig zusammen! In der Vergangenheit klappte es in vielen Einrichtungen eher schlecht als recht, dass vor Einführung neuer Abläufe und Softwareprodukte diese auf ihre organisatorische, rechtliche und technische Sicherheit und Zulässigkeit hin geprüft wurden. Ein wenig halbherzig und zeitlich nachgelagert wurden dann Verfahrensverzeichnisse erstellt, für die sich selten jemand interessierte. Diese beiden Instrumente sollen zukünftig in einer **Datenschutz-Folgenabschätzung** zusammengefasst und dokumentiert werden. Das bedeutet, dass schon in der Planungsphase die datenschutzrechtlichen Folgen geprüft und dokumentiert werden müssen. Eine spätere Erstellung eines Verfahrensverzeichnisses entfällt dann.

2. Geplantes Patientenrechtegesetz

Das geplante Patientenrechtegesetz, das in den neuen §§ 630a ff. BGB Themen wie Patientenaufklärung, Akteneinsicht etc. regeln soll, wurde im Februar vom Deutschen Anwaltsverein kommentiert und durch eine ganze Reihe pragmatischer Vorschläge ergänzt (http://anwaltverein.de/downloads/Stellungnahmen-11/201215-Stellungnahme.pdf)

3. Organspende

Der Bundesdatenschutzbeauftragte Peter Schaar hat Bedenken geäußert, im Rahmen der Einführung der Gesundheitskarte Patienten regelmäßig alle fünf Jahre nach ihrer Bereitschaft zur Organspende zu befragen.

4. BYOD - Bring Your Own Device

Immer mehr Mitarbeiter verwenden im Rahmen ihrer Berufstätigkeit eigene IT-Geräte, insbesondere Smart-Phones. Begründet wird dies häufig damit, dass der Standard am Arbeitsplatz nicht geringer sein soll, als dies die Betreffenden im privaten Bereich gewohnt sind. Diese Einschätzung ist dem Umstand geschuldet, dass betrieblich angeschaffte Hardware frühestens nach den gesetzlich zum Teil sehr lange angesetzten Abschreibungsfristen erneuert wird. Gerade jüngere Mitarbeiterinnen und Mitarbeiter können gerade in ländlichen Gebieten nur noch dann für eine Einrichtung gewonnen werden, wenn diese sich offen im Umgang mit dieser Fragestellung zeigt. Überdies stellt dies auch ein Potential zur Kosteneinsparung dar und kann geeignet sein, die Wettbewerbsfähigkeit zu erhöhen. Datenschutz- und haftungsrechtlich stellt dieser Umstand ein nicht geringes Problem dar, da Zugriffsrechte durchlöchert werden können und das hausinterne Netz mit unwägbaren Gefahren konfrontiert wird.

Hier kann die Flucht nach vorne die Lösung markieren. Statt alles zu verbieten sollten klare Compliance-Regeln angestrebt werden. In Arbeitsverträgen und Betriebsvereinbarungen sollte deutlich geregelt sein, was geht und was nicht und welche Vorsichtsmaßnahmen die Betreffenden zu beachten haben.

5. Fehlende Zugriffsprotokollierung

Ein in den letzten Wochen bekannt gewordenes Urteil des Europäischen Gerichtshof für Menschenrechte v. 28.09.2010 (Application no. 20511/03) rückt die juristische Notwendigkeit der datenschutzrechtlichen Umsetzung der technisch-organisatorischen Maßnahmen in den Vordergrund, wie sie in allen deutschen Datenschutzgesetzen vorausgesetzt werden: fehlende Zugriffsprotokollierungen gehen zu Lasten des Arbeitgebers. Kann nicht geklärt werden, welche Person sich verbotenerweise Zugang zu den Gesundheitsdaten einer HIV-positiven Mitarbeiterin verschafft und diese dann publik gemacht hat, haftet das Krankenhaus als Arbeitgeber.

Den Forderungen der im März 2011 von den deutschen Datenschutzaufsichtsbehörden verabschiedeten Orientierungshilfe Krankenhausinformationssysteme sollte daher zunehmend Rechnung getragen werden.

6. Betriebsrat und betriebliche Eingliederung

Für Arbeitnehmer, die innerhalb eines Jahres länger als sechs Wochen nicht arbeitsfähig sind, ist stets ein betriebliches Eingliederungsmanagement zu prüfen. In einem Beschluss des Bundesarbeitsgerichts hat dieses festgestellt, dass der Betriebsrat ohne Zustimmung des betreffenden Arbeitnehmers den Arbeitgeber überwachen darf, ob dieser seiner Aufgabe nachkommt (http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&sid=16ba38cdb13fc6c623c452e9566d1657&nr=15664&pos=0&anz=1&titel=Betriebliches_Eingliederungsmanagement_-_%DCberwachungsrecht_des_Betriebsrats).

7. Zugriff der Polizei auf Patientendaten verfassungswidrig

Das Bundesverfassungsgericht hat in einem Beschluss Teile des Telekommunikationsgesetzes (https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg12-013.html) für

verfassungswidrig erklärt. Polizei und Nachrichtendienste dürfen nicht das informationelle Selbstbestimmungsrecht, z. B. von Patienten oder Klienten in Krankenhäusern und stationären Einrichten verletzten, indem sie auf Zugangscodes zugreifen können und damit beispielsweise in geschützten WLAN-Netzen Daten erfassen. Gleiches gilt auch für dynamische IP-Adressen.

8. Notfallzugriffe von Ärzten

Der Hamburgische Datenschutzbeauftragte hat im Universitätsklinikum Eppendorf formell beanstandet (http://www.datenschutz-hamburg.de/news/detail/article/ausgestaltung-der-notfallzugriffe-auf-patientendaten-im-uke-formell-beanstandet.html?tx_ttnews%5BbackPid%5D=170&cHash=742c0e9c9482c6e29b339c8979c19353), dass alle Ärzte dort die Möglichkeit haben, mittels eines Notfallzugriffes auf alle elektronischen Patientendaten zugreifen zu können. Bis zu 300 solcher Zugriffe wurden täglich verzeichnet. Diese Rüge unterstreicht die Notwendigkeit eines stringenten Zugriffsrechte- bzw. Rollenkonzeptes der eigenen EDV.

9. Kunden haften für Schäden beim Onlinebanking

Wer auf gefälschte Webseiten herein fällt und dort seine PIN- und TAN-Nummern ein- bzw. preisgibt, bleibt auf seinem Schaden sitzen (http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=dc44466ab878436cf415c3fb6aa329c8&nr=60048&linked=pm&Blank=1). Phising- (Mailaufforderung eine gefälschte Webseite zu besuchen) und Pharming- (auf der gefälschten Webseite die Transaktionsdaten preisgeben) folgen muss nicht die Bank tragen. Der Schaden ist vielmehr vom Kunden zu tragen.

10. Mehr Datenschutz?

Sie möchten gerne weiter lesen? Dann machen Sie etwas Sinnvolles: Vertiefen Sie Ihre Datenschutzkenntnisse mit einem Online-Spiel: http://www.datadealer.net/

Datenschutzkenntnisse gut? Testen Sie sich selbst!

Fragestellung: Unterfallen Pflegekräfte und Verwaltungsangestellte eines Krankenhauses oder einer Suchthilfeeinrichtung auch der ärztlichen, strafbewehrten Schweigepflicht?

Antwort A: Nein, sie sind ja keine Ärzte.

Antwort B: Ja, sie kommen auch mit allen Patienteninformationen in Berührung.

Richtige Antwort ist Nr. B: In § 203 Abs. 3 Satz 2 StGB steht: Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Das heißt: alle in einem Krankenhaus oder einer Suchthilfeeinrichtung arbeitenden nichtärztlichen Personen, die mit Patienteninformationen in Berührung kommen, haben gleichfalls die ärztliche Schweigepflicht zu beachten.

Impressum: Mark Rüdlin – Rechtsanwalt und Datenschutzbeauftragter
Struenseestr. 37 | 22767 Hamburg | Tel. 040 697972 -80 | Fax -90 | mailto: ra@markruedlin.de