Bundesversicherungsamt

Bundesversicherungsamt · Friedrich-Ebert-Allee 38 · 53113 Bonn

An alle
bundesunmittelbaren
gesetzlichen Krankenkassen

nachrichtlich:
GKV-Spitzenverband

HAUSANSCHRIFT Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 (0) 228 619 - 2715
FAX +49 (0) 228 619 - 1858
E-MAIL günter.tscharn@bva.de
INTERNET www.bundesversicherungsamt.de
BEARBEITER(IN) Günter Tscharn

DATUM **05. September 2014**

AZ 715 – 8240 – 2028/2014
(bei Antwort bitte angeben)

- Versand nur per E-Mail -

Rundschreiben zur Sicherung des Online-Portals vor unberechtigten Zugängen und zur Verhinderung unbefugter Zugriffe auf Patientendaten im Rahmen der Patientenquittung gem. § 305 Abs. 1 SGB V

Sehr geehrte Damen und Herren,

wie die Rheinische Post in ihrer Ausgabe vom 26. Juni 2014 berichtete, ist es einer Testperson gelungen, sich mittels sog. Identitätsdiebstahl unbefugt Zugang zu Patientendaten über das Online-Portal einer Krankenkasse zu erschleichen. Eine daraufhin von uns durchgeführte Stichprobenanalyse hat ergeben, dass sowohl die einmaligen Registrierungsverfahren für eine Nutzung von Online-Dienste als auch die dann regelmäßigen Identitätsprüfungen bei Anmeldung an den Portalen in der Praxis sehr unterschiedlich gehandhabt werden. Unabhängig von weiteren möglichen Prüfungen der Aufsicht bzw. des Prüfdienstes unseres Hauses, weisen wir Sie mit diesem Schreiben auf unseres Erachtens unabdingbare Sicherheitsaspekte hin.

Zunächst ist es aus unserer Sicht unstrittig, dass die unterschiedlichen online angebotenen Dienste hinsichtlich des erforderlichen Schutzbedarfs individuell und differenziert zu betrachten sind. Nur auf Grundlage individueller Risikoanalysen kann die Wirksamkeit von Sicherheitsmaßnahmen beurteilt werden. Wir raten den Kassen daher eindringlich, die möglichen Gefahren der online angebotenen Dienstleistungen und zur Verfügung gestellten Prozesse im Hinblick auf die Sensibilität der zu übermittelnden Daten differenziert im Einzelnen zu analysieren und entsprechende technische und organisatorische Schutzmaßnahmen zu formulieren. Der Sicherheitsprozess sowie die Abwägungen müssen nachvollziehbar dokumentiert sein. Methodische Hinweise auf eine solche Risikoanalyse sowie eine Darstellung möglicher Maßnahmen gibt das Bundesamt für Sicherheit in der Informationstechnik (siehe hierzu ausführlich www.bsi.de unter dem Schlagwort „IT-Grundschutz").

Darüber hinaus ist zu beachten, dass in einigen Anwendungsfällen die Sicherheitshürden sehr hoch anzusetzen sind, vor allem, wenn besonders schutzbedürftige personenbezogene Daten wie zum Beispiel Gesundheitsdaten betroffen sind (§ 67 Abs. 12 SGB X). Wie auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nahezu regelmäßig in ihrem Tätigkeitsberichten ausführt, sind in solchen Verfahren die höchsten Verschlüsselungs- und Authentifizierungsstandards einzusetzen. Zum Beispiel dürfen Gesundheitsdaten nicht per DE-Mail versendet werden, obwohl das E-Government-Gesetz die DE-Mail in bestimmten Anwendungsfällen als mögliches Sicherheitsinstrument ansieht (siehe § 36a Abs. 2 SGB I und vgl. dazu BfDI: Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels DE-Mail, Bonn, 01. März 2013).[1]

Vor diesem Hintergrund versteht es sich von selbst, dass die hoch sensiblen Gesundheitsdaten in der sog. Patientenquittung gem. § 305 Abs. 1 SGB V eines besonderen Schutzes bedürfen. Nach unseren aktuellen Einschätzungen dürften solche Informationen nicht ohne

- einen sicheren Registrierungsprozess mit Identitätsnachweis,
- eine Authentisierung am Online-Portal mittels sicherem Identitätsnachweis gem. § 36a Abs.2 SGB I und
- geeignete Verschlüsselungstechniken hinsichtlich der Übertragung

online zur Verfügung gestellt werden.

Wir bitten Sie daher eindringlich, die bei Ihnen umgesetzten Verfahren darauf hin zu überprüfen und ggf. Online-Dienste wie die Patientenquittung gem. § 305 Abs. 1 SGB V bis zur sicherheitstechnischen Revision vorsorglich nicht mehr online anzubieten.

Mit freundlichen Grüßen
Im Auftrag

(Günter Tscharn)

[1] Quelle: http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailHandreichung.pdf?__blob=publicationFile, Zugriff: 03.09.2014.