Anlage 2 zur V E R E I N B A R U N G zwischen dem Verband der Privaten Krankenversicherung e.V. und dem Bundesversicherungsamt nach § 51 Absatz 1 Satz 3 SGB XI vom 27. November 2017

Sicherheitskonzept

Zur sicheren Nutzung des FTP-Servers des Bundesversicherungsamtes sind folgende Regelungen einzuhalten.

(1) Das Bundesversicherungsamt und der Verband der Privaten Krankenversicherung e. V. vereinbaren Kommunikationswege und Ansprechpartner, über die benötigte Informationen zur Benutzerverwaltung ausgetauscht werden (bspw. Benutzer anlegen oder löschen, Zurücksetzen von Passwörtern) sowie zu sonstigen Angelegenheiten den FTP-Server betreffend und zum Austausch kryptographischer Schlüssel.

(2) Der Verband der Privaten Krankenversicherung e.V. muss,
- nicht mehr aktive Benutzer unverzüglich dem Bundesversicherungsamt melden.
- Passwörter für den Zugang zum FTP-Server geheim halten bzw. sicher aufbewahren wenn nötig.
- Passwörter für den Zugang zum FTP-Server bei Verdacht auf Offenlegung unverzüglich ändern bzw. vom Bundesversicherungsamt ändern lassen.
- Passwörter für den Zugang zum FTP-Server regelmäßig ändern bzw. vom Bundesversicherungsamt ändern lassen, so dass das neue Passwort nicht aus dem alten Passwort abgeleitet werden kann (z. B. mittels durchzählen).
- bei Verbindungsaufbau das SSL-Zertifikat oder den öffentlichem SSH-Schlüssel des Servers prüfen. Es dürfen keine Daten auf dem FTP-Server ablegt werden, wenn die Prüfung fehlt schlägt. Vorfälle dieser Art sollen dem Bundesversicherungsamt über die vereinbarten Kommunikationswege gemeldet werden.

(3) Das Bundesversicherungsamt stellt sicher,
- dass nicht mehr aktive Benutzer unverzüglich deaktiviert werden.
- dass sichere Mechanismen für das Zurücksetzen von Passwörtern eingesetzt werden.
- dass die Aktivierung neuer öffentlicher SSH-Schlüssel des FTP-Servers sowie neuer Schlüssel für die Inhaltsverschlüsselung unverzüglich über die vereinbarten Kommunikationswege an die Pflegeversicherungsunternehmen gemeldet wird.
- dass nur vom BSI als sicher eingestufte Kryptoalgorithmen eingesetzt werden und privates kryptographisches Schlüsselmetrial sicher erzeugt und aufbewahrt wird.

- dass bei (Verdacht auf) Kompromittierung eines privaten Schlüssels, dieser nicht mehr eingesetzt wird und eine Mitteilung sowie Verteilung neuer gültiger Schlüssel über die vereinbarten Kommunikationswege erfolgt.

Der Verband der Privaten Krankenversicherung e.V. und das Bundesversicherungsamt nutzen die Kommunikationswege unter (1), um sich gegenseitig darüber in Kenntnis zu setzen, wenn technische Störungen festgestellt worden sind, die eine Übermittlung der Meldedaten an das Bundesversicherungsamt verhindern können. Der Verband der Privaten Krankenversicherung e.V. informiert das Bundesversicherungsamt unverzüglich über Maßnahmen und die voraussichtliche Dauer für die Behebung der Störung. Sofern es sich um technische Störungen bei dem Verband der Privaten Krankenversicherung e. V. oder dessen Mitgliedsunternehmen handelt, ist sicherzustellen, dass die Meldungen dem Bundesversicherungsamt in der im § 4 der Vereinbarung benannten Form umgehend nach Behebung der Störung gemäß § 5 der Vereinbarung übermittelt werden. Nur in diesem Fall sind die Meldefristen nach § 3 der Vereinbarung als erfüllt zu erachten. Dies gilt entsprechend bei technischen Störungen auf Seiten des Bundesversicherungsamtes.