Anhang B Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit bei der Auftragnehmerin (HÄVG RZ AG)

Zu den Regelungstatbeständen des § 295 Abs. 1 b Satz 6 SGB V in Verbindung mit § 78a SGB X werden folgende technische und organisatorische Maßnahmen festgelegt:

1. Zutrittskontrolle:

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen der HÄVG RZ AG, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt:

Die Gebäude der HÄVG RZ AG an den Standorten Köln und Haan, in denen personenbezogene Daten verarbeitet werden, sind nicht frei zugänglich, sondern durch Zutrittskontrollen gesichert. Die Gebäude sind jeweils nach außen hin eine geschlossene Einheit. Die Zutrittskontrolle erfolgt zum einen über die Begrenzung der möglichen Zutrittsmöglichkeiten (Vorder- und Hintereingang mit personenbezogenen Schlüsselchips bzw. personenbezogenen Schlüsselkarten). Die Tiefgarage am Standort Köln ist ebenfalls nur mit personenbezogenem Schlüsselchip zu betreten und zu verlassen und durch ein Rolltor zusätzlich abgeschottet und zum weiteren durch den Pförtnerdienst am Vordereingang gesichert. Ohne einen personenbezogenen Schlüsselchip oder eine personenbezogene Schlüsselkarte, die jeweils nur den Mitarbeitern der HÄVG RZ AG zur Verfügung gestellt ist, ist daher der Zutritt zu den Gebäuden nur durch Pförtnereinlass möglich. Die Ausgabe der Schlüsselchips und Schlüsselkarten wird schriftlich dokumentiert. Die Mitarbeiter sind verpflichtet, den Verlust von Chip oder Karte unverzüglich zu melden, damit diese über das jeweilige Zutrittskontrollsystem gesperrt werden.

Der hintere Teil des Gebäudes am Standort Köln ist eingezäunt incl. der Parkplätze für die Mitarbeiter (Rollgitter). Das Rollgitter wird außerhalb der normalen Dienstzeiten verschlossen. Anhand einer Videoanlage wird mit zwölf verschiedenen Kameras die Außenhaut und die hausinterne Tiefgarage überwacht. Das Bild dieser Kameras wird wahlweise auf einen Monitor beim Pförtner aufgeschaltet.

Im hinteren Teil des Gebäudes am Standort Haan erhalten speziell autorisierte Fremddienstleister, die verschlüsselte Daten (CDs für Offline-Abrechnung) anliefern, Zutritt nur durch eine separate, speziell gesicherte Zugangsschleuse, die getrennt von dem anderen Zugang ist.

Besucher und sonstige Fremddienstleister erhalten ausschließlich Zutritt über den Vordereingang. Die Anwesenheit dieser Personen wird schriftlich in Listen beim Pförtner notiert, die Personen werden von Mitarbeitern der HÄVG RZ AG beim Pförtner in Empfang genommen und bewegen sich im Gebäude nur in Begleitung eines Mitarbeiters und werden von diesem auch wieder zum Pförtner begleitet. Die Abwesenheit wird schriftlich vermerkt.

Außerhalb der Dienstzeiten sind die Gebäude durch einen aufgeschalteten Direktalarm zu einem privaten Sicherheitsdienst alarmgesichert. Die Überwachung erfolgt durch Bewegungsmelder in den Gebäuden inkl. nächtlicher Bestreifung.

Mitarbeitern der HÄVG RZ AG wurden separate Türschlüssel zu ihren Büros ausgehändigt und der Empfang der Schlüssel von den Mitarbeitern quittiert. Mitarbeiterausweise mit Lichtbild wurden erstellt und ausgehändigt. Das Tragen während der Dienstzeit wurde angewiesen.

Die Schlüssel zu den Räumlichkeiten, in denen die Auftragsdaten verarbeitet bzw. vernichtet werden, befinden sich in der ausschließlichen Obhut der Geschäftsleitung der HÄVG RZ AG sowie ggf. der zuständigen Mitarbeiter. Dritte haben zu den Räumlichkeiten keinen Zutritt. Die Vergabe von Schlüsseln ist schriftlich geregelt.

Der Zutritt zu weiteren Gebäudeteilen muss durch den Pförtner autorisiert werden, da dieser zusätzlich alarmgesichert ist. Hierbei wird ebenfalls die Schlüsselausgabe und -Rückgabe zu diesem Gebäudeteil beim Pförtner schriftlich festgehalten.

Der Zutritt zum fensterlosen, klimatisierten Serverraum ist doppelt gesichert (Chip und Generalschlüssel, Schlüssel wird im separaten Schlüsseltresor im IT-Bereich durch vierstelligen Zahlencode gesichert, zu dem nur die zuständigen Mitarbeiter Zugang haben). Zugang haben nur die zuständigen Mitarbeiter. Die Türen zum Serverraum bestehen aus Metall. Die Serverracks werden durch die IT-Administration stets verschlossen gehalten. Die EDV-Anlage der HÄVG RZ AG besteht aus Hardware-Komponenten der Hersteller IBM und HP, Betriebssysteme sind Windows 2003 bzw. Windows 2008 jeweils R2, Anwendungssoftware ist Microsoft Exchange.

Von allen Mitarbeitern der HÄVG RZ AG und kontinuierlich tätigen Fremddienstleistern (z. B. Reinigungspersonal) liegen Datenschutzerklärungen auf der Grundlage von § 5 BDSG sowie § 35 SGB I vor.

2. Zugangskontrolle

Durch geeignete Sicherheitsmaßnahmen wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich über eine SSL gesicherte Verbindung (Webservice) mit Client-Authentifizierung. Zugang haben nur registrierte Benutzer, die sich über Benutzername und Passwort authentifizieren müssen.

Es bestehen detaillierte Regeln für die Passwortvergabe, die bei der Neuvergabe von Passwörtern jeweils automatisiert geprüft werden. Ein Passwort muss mindestens acht Zeichen lang sein. Es darf nicht Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen. Das Kennwort muss drei von vier Kriterien erfüllen: mind. einen Großbuchstaben, mind. einen Kleinbuchstaben, mind. ein nicht

alphanumerisches Zeichen. Ein Kennwortwechsel ist spätestens nach 90 Tagen erforderlich und wird im System erzwungen. Es müssen drei neue, gültige Kennwörter erstellt worden sein, ehe ein bereits einmal verwendetes Kennwort erneut genutzt werden kann.

Der Umfang der Rechte einzelner Nutzer ist individuell oder auf Gruppenbasis individuell beschränkt. Für bestimmte Sicherheitsstufen (z.B. Administratorrechte - Systemsteuerung) sind evtl. zusätzliche Passworte erforderlich.

Es werden Firewalls (Perimeterschutz) der Marke Cisco Systems und Check Point eingesetzt, um eine Umgehung bzw. Durchdringung der Zugangskontrollmechanismen bei vernetzten Systemen zu verhindern. Die Kommunikation der verschiedenen Systeme und Standorte erfolgt über VPN End-to-End Verbindung. Die Firewall lässt durch das VPN nur bestimmte Protokolle z. B. RDP und Citrix zu.

3. Zugriffskontrolle

Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Der Zugriff auf das System ist mit Benutzerkennungen und (abgestuften) individuellen Passwörtern geschützt. Für Fernwartungstechniker besteht eine gesonderte USER-ID, die keine Einblicke in Dateien mit personenbezogenen Daten zulässt. Ein Virenscanner der Marke Symantec Endpoint Protection ist installiert, der zusätzlich auch als Datenschutz-Software eingesetzt wird.

Über ein abgestuftes Rollen/Rechte-Konzept werden nur die notwendigen Daten zugänglich gemacht, welche dem Arbeitsgebiet des Benutzers entsprechen und zur Ausübung der zugewiesenen Tätigkeit unbedingt erforderlich sind.

Die entsprechenden Rollen und Rechte werden zentral administriert, überwacht und protokolliert. Für die Beantragung, Änderung und Löschung von Berechtigungen werden formulargesteuerte, revisionssichere Verfahren eingesetzt. Bei der praktischen Umsetzung wird zwischen Antragsteller, Genehmiger und Einrichter differenziert. Es ist nicht zulässig, dass ein Mitarbeiter der HÄVG RZ AG in diesem Verfahren zwei Funktionen inne hat.

Das Datenverarbeitungssystem enthält eine automatische Sperrung, die nach drei fehlerhaft eingegebenen Passwörtern erfolgt. Es werden Bildschirmschoner eingesetzt, die sich nach 15 Minuten Inaktivität automatisch aktivieren und nur durch Eingabe des Benutzerpassworts wieder deaktiviert werden können.

Der direkte Zugriff auf die sensiblen Daten im Rahmen dieses Auftragsverhältnisses wird immer protokolliert und beinhaltet eine entsprechende Historisierung. Die externe Speicherung (Auslagerung, Backup, Daten für Transfer) von diesen Daten erfolgt nur durch die berechtigten IT-Administratoren und ist auch nur diese möglich. Eine unbefugte Nutzung der USB-Ports der Server ist durch abgeschlossene Racks, Raumsicherungsmaßnahmen und das benötigte Administrator-Passwort ausgeschlossen. Daten auf allen Datenträgern dürfen stets nur in verschlüsselter Form gespeichert werden.

Datenträger werden sorgfältig aufbewahrt, in verschlossenen Behältnissen in einem abgeschlossenen Schrank im Rechenzentrum (Sicherungsmaßnahmen analog zu Servern).

Personenbezogene Daten werden in physischer Form (Datenträger, Papier) über eine abgeschlossene Aktenvernichtungstonne mit nachfolgender datenschutzkonformer Vernichtung durch ein zertifiziertes Fachunternehmen entsorgt.

4. Weitergabekontrolle

Die HÄVG RZ AG stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Sozialdaten werden nur über die mit SSL oder anderen Verfahren mit vergleichbaren Sicherheitsstandards (z.B. digitaler Signatur nach PEM bzw. PKCS7-Standard, PGP) gesicherte und Client-Authentifizierte Verbindung übertragen. Es werden zusätzlich verschlüsselte Leitungen (End-to-End-Verschlüsselung) verwendet. Die Systeme sind mit Firewalls gesichert. Die Serversysteme sind zudem über Intrusion Detection Systeme abgesichert. Sämtliche Datenübertragungswege sind fest konfiguriert bzw. programmiert, so dass sie vom Anwender selbst nicht ausgewählt oder eingestellt werden können.

Eine Dokumentation der verschlüsselten Übertragungswege von verschlüsselten personenbezogenen Sozialdaten wird in einem Dokumentenmanagementsystem (Auto-Q-Manager), so dass überprüft und festgestellt werden kann, an welche Stelle eine Übermittlung vorgenommen wird.

Die zur Erfüllung des Auftrags notwendige Datenübermittlung an die Krankenkasse erfolgt nur im Rahmen von vertraglichen Vereinbarungen, durch autorisierte Personen, nach Rücksprache mit dem Verantwortlichen für Datenschutz und unter Einsatz besonderer Sicherungsmaßnahmen (z.B. digitaler Signatur nach PEM bzw. PKCS7-Standard, PGP).

Datenträger werden grundsätzlich in verschließbaren Transportbehältern transportiert. Sofern Daten auf CD übermittelt werden, werden die Daten vor dem Brennen auf die CD verschlüsselt.

In den Feldern der übertragenen Datei werden Angaben zum Erstellungszeitpunkt und zur Person des Erstellers vermerkt.

5. Eingabekontrolle

Die HÄVG RZ AG gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Der Zugriff auf die Daten erfolgt ausschließlich durch authentifizierte Benutzer und im Rahmen derer autorisierter Rechte. Zugriffe auf Sozialdaten werden unter Angabe von Datum, Uhrzeit und Benutzerkennung im System der HÄVG RZ AG protokolliert. Die Protokollierung erfolgt innerhalb der Programme zur Dateneingabe, -verarbeitung und -löschung durch Abspeichern des jeweiligen Vorgangs automatisch. Die Protokollierung erfolgt in einer separaten Datenbank.

Die Protokolle zur Eingabe, Veränderung und Löschung enthalten folgende Angaben:

- Authentifizierter Benutzer
- Datum und Uhrzeit der Eingabe, Veränderung und Löschung
- Originaldatum vor Eingabe, Veränderung und Löschung
- Eingegebener Datensatz, verarbeiteter Datensatz, Gelöschtkennzeichnung

Zugriff auf die Protokollierungen haben seitens der HÄVG RZ AG nur zwei vom Vorstand der HÄVG RZ AG bestimmte Personen, die die Protokollierungen stichprobenhaft monatlich überprüfen. Die Auftraggeberin kann die Protokollierung jederzeit einsehen. Für die Protokolle gelten dieselben Aufbewahrungsfristen wie für die personenbezogenen Daten gemäß § 4 des Auftrages.

Die HÄVG RZ AG stellt sicher, dass ausschließlich korrekte Daten der eingeschriebenen Patienten von Ärzten, die an der hausarztzentrierten Versorgung teilnehmen, in die Abrechnungsdatenverarbeitung übernommen werden. Hierzu werden Testsysteme und pseudonymisierte Testdatensätze zur Überprüfung von Eingabedaten erstellt. Die Testergebnisse werden im 4-Augen-Prinzip fachlich validiert. Es werden Plausibilitätskontrollen durchgeführt.

6. Auftragskontrolle

Die HÄVG RZ AG stellt sicher, dass personenbezogene Daten im Auftrag nur von eigenen Mitarbeiterinnen und Mitarbeitern nur gemäß den Weisungen der Krankenkasse verarbeitet werden. Unterauftragnehmer werden für die HÄVG RZ AG im Rahmen dieses Auftragsverhältnisses nicht tätig.

Der Auftraggeber ist jederzeit berechtigt, sich in den Geschäftsräumen der HÄVG RZ AG von der ordnungsgemäßen Verarbeitung der personenbezogenen Daten sowie von der Einhaltung der bei der HÄVG RZ AG vor Ort getroffenen technischen und organisatorischen Datensicherungsmaßnahmen zu überzeugen.

Die HÄVG RZ AG ist verpflichtet, die Verarbeitung der ihr übergebenen personenbezogenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers durchzuführen (§ 11 BDSG). Ist die HÄVG RZ AG der Ansicht, dass eine Weisung des Auftraggebers gegen das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat sie den Auftraggeber unverzüglich darauf hinzuweisen.

Die HÄVG RZ AG ist verpflichtet, dem Auftraggeber jederzeit ***Auskünfte*** zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Nicht mehr erforderliche Daten sind bei der HÄVG RZ AG unverzüglich zu löschen.

Bei Beendigung des Auftragsverhältnisses verpflichtet sich die HÄVG RZ AG, alle ihr in Zusammenhang mit dem Auftrag übergebenen und bis dahin noch nicht verarbeiteten bzw. gelöschten personenbezogenen Daten an den Auftraggeber zurückzugeben bzw. den Nachweis einer ordnungsgemäßen Vernichtung darüber zu führen.

Das zugrunde liegende Auftragsverhältnis regelt detailliert den Auftragsinhalt (s. insbesondere Anhang A Leistungsbeschreibung) und räumt der Krankenkasse Kontrollrechte und -pflichten ein. Die Kriterien zur Auswahl der HÄVG RZ AG ergeben sich aus § 80 Abs. 5 Nr. 1 SGB X.

7. Verfügbarkeitskontrolle

Die HÄVG RZ AG gewährleistet, dass an beiden Standorten in Köln und in Haan personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Die Daten werden nach einem Generationsprinzip auf Band gesichert, in einem brandsicheren Safe und separatem Raum gelagert und zusätzlich als Datenbankreplikat vorgehalten. Weitere Maßnahmen sind die redundante Auslegung der IT-Systeme, incl. Stromversorgung, Backups, Schutzmaßnahmen ggf. sog. Schadsoftware und Vorkehrungen zum Brandschutz.

Es besteht für die HÄVG RZ AG für beide Standorte Köln und Haan ein Notfallplan für einen angemessenen organisatorischen Umgang mit der Bedrohung des Geschäftsbetriebs. Der Plan regelt die Einbeziehung von Rollen und Gremien in den Prozess, die Definition des Krisenstabs, die Notfalldefinition und die für eine schnellstmögliche Wiederaufnahme der Auftragsverarbeitung erforderlichen, konkreten Maßnahmen.

8. Trennungsgebot

Die HÄVG RZ AG stellt sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Abschottung der Datenbestände wird durch Speicherung in getrennten physischen Dateien bzw. Datenbanken erreicht. Über das in Nr. 3 (Zugriffskontrolle) erwähnte Rollen- und Rechte-

Konzept enthalten Anwender nur auf die Daten Zugriff, die für das jeweilige Arbeitsgebiet notwendig sind. Eine Zusammenführung der getrennten Daten wird durch die Rechtevergabe im Rahmen der Zugangs- und Zugriffskontrolle verhindert.

Die Entwicklungs-, Test- und Produktionsumgebung sind voneinander getrennt. Die Testumgebung hat nur eine eingeschränkte Verbindung zum Produktionsnetz. Aus der Entwicklungsumgebung ist kein Zugriff auf die Testumgebung, aus der Testumgebung ist kein Zugriff auf die Produktionsumgebung möglich. Produktionsdaten kommen nicht mit Entwicklungsumgebungen in Berührung.

Der Verwendungszweck der einzelnen Umgebungen ist klar definiert. Funktionstests finden nur in der Entwicklungsumgebung statt, fachliche Funktionstests und Fehlersuche finden ausschließlich in der Testumgebung statt, in der Produktionsumgebung finden keine Tests statt.

Für die datenschutzgerechte Vernichtung von Fehldrucken und sonstigem Datenmüll stehen Container der Marke shred-it zur Verfügung, die einen Zugriff auf die in den Containern enthaltenen Unterlagen/Daten nach Einwurf nicht mehr ermöglichen.

Die Daten unterschiedlicher Auftragnehmer werden im Rahmen einer Mandantenlösung und damit verbundener differenzierter Zugriffsrechte voneinander abgeschottet.