Technisch Organisatorische Maßnahmen

PVZ Ecker Allgemeinmediziner GmbH

Goethestraße 12
4614 Marchtrenk
Österreich

1. Technische Maßnahmen hinsichtlich Benutzer

1.1. Bildschirmsperre

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer verpflichtet sind, beim Verlassen des Arbeitsplatzes den Computer so zu sperren, dass er durch Dritte nicht genutzt werden kann (Stichwort: Bildschirmsperre). Es sind sämtliche Geräte so einzustellen, dass eine Bildschirmsperre nach spätestens 10 Minuten Nichtbenut-zung des Computers diesen automatisch sperrt, sodass dieser erst wieder nach Eingabe eines Kennworts verwendet werden kann.

1.2. Clean Desk Policy

Beschreibung:

Der Verantwortliche stellt sicher, dass jeder Mitarbeiter sich verpflichtet, Dokumente und Unterlagen vor Verlassen des Arbeitsplatzes entsprechend zu verstauen und einzuschließen, sodass ein unbefugter Dritter keinerlei Kenntnis über deren Inhalt erhalten kann. Das „Aufräumen und Abschließen“ beinhaltet sämtliche Unterlagen, Datenträger und sonstige Informationsmedien.

1.3. Eingeschränkter Zugang zum Emailsystem

Beschreibung:

Der Zugang zum Emailsystem (Outlook)
Ist nur nach Eingabe von Benutzername und Passwort möglich

1.4. Eingeschränkter Zugang zur Buchhaltungssoftware

Beschreibung:

Der Zugang zur Buchhaltungssoftware ist nur für jene Mitarbeiter möglich, die die Buchhaltung durchführen. Zusätzlich werden Patientenrechnungs Kopien an den Steuerberater in Papierform übermittelt.

1.5. Eingeschränkter Zugang zur Patientenverwaltung

Beschreibung:

Der Zugang zum Patientenverwaltungssystem (CGM PC po) ist nur nach Eingabe von Benutzername und Passwort möglich

1.6. Geeigneter Umgang mit Laufwerken für Wechselmedien und externe Datenträger (Handhabung, Entsorgung, Transport)

Beschreibung:

Den Mitarbeitern ist es ohne explizite Erlaubnis nicht gestattet, personenbezogene Daten, die der Verantwortliche verarbeitet, auf Datenträger zu speichern. Eine solche Speicherung wird der jeweilige Verantwortliche explizit anordnen und – für den Einzelfall – geeignete Sicherheitsmaßnahmen anordnen.

1.7. Keine Datenspeicherung auf den Arbeitsplatzrechnern

Beschreibung:

Auf den Arbeitsplatzrechnern selbst werden keine zu sichernden Daten abgelegt. Alle Daten werden entweder über die Praxis-Software des Verantwortlichen erfasst und somit in der zentralen Datenbank gespeichert, oder auf einem – je nach Berufsgruppe – bereitgestellten Netzwerklaufwerk abgelegt.

1.8. Sichere Nutzung des Internets

Beschreibung:

Der Verantwortliche stellt sicher, dass Benutzer eine Schulung zum sicheren Umgang mit dem Internet erhalten. Die Schulung der Mitarbeiter erfolgt einmal im Jahr.

1.9. Sicherer Umgang mit Speichermedien

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Computer so gesperrt sind, dass Speichermedien nur nach Eingabe eines Passworts verwendet werden können. USB-Ports werden gesperrt.

1.10. Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Arbeitsplatzrechner so gesichert sind, dass Rechnermikrofone und Kameras gegen unberechtigten Zugriff gesperrt sind. Sämtliche Arbeitsplatzrechner erhalten regelmäßig Sicherheitsupdates und werden regelmäßig auf Viren untersucht. Die Grundkonfiguration der Rechner sieht vor, dass die Rechner vor unberechtigtem Zugang geschützt sind (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

1.11. Verwendung einer Passwort Richtlinie

Beschreibung:

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist, wobei Passwörter gewisse Kriterien erfüllen müssen (Passwortrichtlinie hinsichtlich minimaler Länge und Sonderzeichen).

Risiken:

Zugriff von unberechtigten Personen

Verhaltensregeln:

Verwendung sicherer Passwörter, keine Weitergabe von Passwörtern

1.12. Zugangsschutz Mailserver

Beschreibung:

Der Zugang zum Mailservice ist nur mit Passwort möglich

2. Organisatorische Maßnahmen hinsichtlich Benutzer

2.1. Abschluss von Geheimhaltungsvereinbarungen

Beschreibung:

Der Verantwortliche stellt sicher, dass mit sämtlichen Mitarbeitern eine Geheimhaltungsvereinbarung mit folgendem Inhalt geschlossen worden ist:

„Der Dienstnehmer ist verpflichtet, personenbezogene Daten aus Datenverarbeitungen, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anver-traut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (kurz: das Datengeheimnis).

Dienstnehmer dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung des Dienstgebers übermitteln.

Das Datengeheimnis besteht auch über das Ende des Dienstverhältnisses hinaus unbefristet fort.“

Risiken:

Geheimnisoffenbarung, kein Unrechtsbewusstsein zum Datenschutz

Verhaltensregeln:

Verpflichtung zum Abschluss einer Geheimhaltungsvereinbarung

2.2. Durchführung regelmäßiger Mitarbeiterschulungen

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter regelmäßig geschult werden. Im Rahmen der Schulung werden die Mitarbeiter aufgeklärt, auf welche Art und Weise personenbezogene Daten verarbeitet werden dürfen und welche Daten-sicherheitsmaßnahmen zu ergreifen sind. Der Verantwortliche stellt sicher, dass ein entsprechender Nachweis der Schulung im Personalakt des jeweiligen Mitarbeiters abgelegt wird. Im Rahmen der Schulung werden die Mitarbeiter auch über die sichere Nutzung von Browsern, die sichere Nutzung von sozialen Netzwerken sowie über die Zulässigkeit der Nutzung von Kommunikationsmedien informiert. Der Verantwortliche hat seine Mitarbeiter darüber aufgeklärt, dass die Nutzung von Onlinespeichern („Cloud-Dienste“) – ohne ausdrückliche Genehmigung des Verantwortlichen – nicht zulässig ist. Die Mitarbeiter werden dahingehend geschult, dass diese umgehend bekannt geben müssen, sollte ein genutztes Endgerät – egal aus welchem Grund – nicht mehr nutzbar sein (Defekt, Verlust, Diebstahl).

2.3. Elektronische Zeiterfassung mittels Chip

Beschreibung:

Elektronische Zeiterfassung mittels Chip und Lesegeräten die Bit Factory = Auftragsverarbeiter

2.4. Mitarbeiter-Austritt Prozess (Organisationshandbuch)

Beschreibung:

Der Verantwortliche stellt sicher, dass Benutzer gelöscht oder gesperrt werden, so-bald diese keinen Zugriff mehr auf das System benötigen (etwa: Löschen von Benut-zer-Konten von ehemaligen Mitarbeitern).

2.5. Nutzung von Kommunikationsmitteln und Klassifizierung von Dokumenten nach Vertraulichkeitsstufen

Beschreibung:

Der Verantwortliche klassifiziert Dokumente wie folgt:

1. Vertraulich
2. Nicht vertraulich
3. Öffentlich bekannt

Der Verantwortliche nutzt folgende Kommunikationsmedien:

1. Persönliche Übergabe
2. Versand per verschlüsselter elektronischer Kommunikation
3. Versand per eingeschriebenem Brief
4. Versand per Post
5. Versand per Fax
6. Versand per E-Mail
7. Telefonische Mitteilung
8. Versand per SMS
9. Versand per Messenger Dienst (etwa: Whatsapp)

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Vertraulich - Persönliche Übergabe, Versand per verschlüsselter elektronischer Kommunikation, Versand per Post
Nicht vertraulich - Jedes Medium
Öffentlich bekannt - Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Informationen, die die Sozialversicherungsnummer enthalten - Vertraulich
Gesundheitsdaten - Vertraulich
Adressinformationen - Vertraulich
Kontaktinformationen - Vertraulich
Informationen über Patienten - Vertraulich
Befunde - Vertraulich

Die Weitergabe von Zugangsdaten und Passwörtern im Zusammenhang mittels ver-schlüsselter elektronischer Kommunikation erfolgt ausschließlich per Post, persön-lich oder per SMS (nach vorheriger schriftlicher Einwilligungserklärung des Empfän-gers).

Zulässige Kommunikationsmedien:

Der Arzt als datenschutzrechtlicher Verantwortlicher wird vertrauliche Informationen (etwa Gesundheitsdaten und Befunde) an Patienten mittels unverschlüsselter E-Mail nur senden, wenn der jeweilige Patient vorab in die unverschlüsselte Zusendung eingewilligt hat. Sollte keine schriftliche Einwilligung des Patienten vorliegen, hat der Arzt als datenschutzrechtlicher Verantwortliche die mündliche Einwilligung des Patienten in der Patientenakte zu dokumentieren.

Der Verantwortliche verpflichtet sich, vertrauliche Informationen (etwa Gesundheitsdaten) an zulässige Übermittlungsempfänger (etwa: Apotheken, Ärzte, Krankenhäuser, Pflegeheime, Krankenversicherungen) ausschließlich mittels verschlüsselter elektronischer Kommunikation oder mittels Fax zu senden.

2.6. Regeln zum Verlassen der Räumlichkeiten

Beschreibung:

Der Verantwortliche stellt sicher, dass die Mitarbeiter dahingehend geschult werden, dass sämtliche Fenster und Türen bei Verlassen der Räumlichkeiten geschlossen bzw. abgeschlossen werden, sodass ein unbefugter Dritter keinen Zugang zu den

Räumlichkeiten des Verantwortlichen bzw. zu personenbezogenen Daten hat. Dies ist im Organisationshandbuch (siehe Enns) festgelegt.

Risiken:

Zugang unbefugter Personen

Verhaltensregeln:

Schließen von Fenster und Türen beim Verlassen von Räumlichkeiten

2.7. Sicherung von physischen Dokumenten

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter dahingehend geschult werden, dass Dokumente der Kategorie „vertraulich“ in einem verschlossenen Aktenordner oder Aktenschrank verwahrt und unmittelbar nach dem Gebrauch wieder eingeschlossen werden müssen. Der Verantwortliche hat mit den Mitarbeitern geeignete Maßnahmen zur Sicherung des Schlüssels getroffen.

Risiken:

Zugriff und Einsicht auf Daten von unberechtigten Personen

Verhaltensregeln:

Vertrauliche Dokumente sind in einem verschlossenen Aktenordner oder -schrank zu verwahren

2.8. Verbot zu Bring your Own Device (BYOD)

Beschreibung:

Der Verantwortliche hat die Verwendung von eigenen Endgeräten (Smartphone, Tablets, Laptops) generell untersagt.

Risiken:

Zugriff unbefugter Personen, Datenverlust

Verhaltensregeln:

Keine Mitnahme eigener Endgeräte

2.9. Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer sich verpflichten, sich nach dem Erfüllen einer Aufgabe vom jeweiligen Arbeitsplatzrechner abzumelden.

3. Technische Maßnahmen hinsichtlich IT-Infrastruktur

3.1. Durchführung von Softwaresicherheitsmaßnahmen

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Endgeräte regelmäßig mit Updates versorgt werden und Softwarepakete, welche Sicherheitslücken schließen, automa-tisch und regelmäßig in die entsprechenden Systeme eingespielt werden. Er stellt darüber hinaus sicher, dass regelmäßig geprüft wird, ob das Einspielen ordnungsgemäß funktioniert hat. Der Verantwortliche stellt sicher, dass Backups der Datenbestände in regelmäßigen Abständen erstellt werden.

Risiken:

Datenverlust

3.2. Elektronische Datenübermittlung per End-zu-End Verschlüsselung

Beschreibung:

Die elektronische Datenübertragung zwischen Labor und Verantwortlichem erfolgt über DaMe und ist End-zu-End verschlüsselt.

3.3. Sichere Verwendung der Arbeitsplatzrechner

Beschreibung:

Der Verantwortliche stellt sicher, dass Computer vor unbefugtem Zugriff und unbefugter Nutzung geschützt sind. Darüber hinaus sind sämtliche Arbeitsplatzrechner so konfiguriert, dass sich Updates und Softwarekorrekturen, die Sicherheitslücken schließen, automatisch installieren. Bei Arbeitsplatzrechnern, auf denen besondere Kategorien von Daten gespeichert sind, sind die genutzten Speichermedien verschlüsselt.

3.4. Sichere Verwendung von Mobiltelefonen

Beschreibung:

Sofern auf mobilen Endgeräten (Mobiltelefone, Tablets oder Ähnliches) personenbe-zogene Daten gespeichert werden, wird der Verantwortliche Maßnahmen dahinge-hend ergreifen, dass der Zugriff auf die mobilen Endgeräte erst nach Eingabe eines Kennworts möglich ist. Mobile Endgeräte sind darüber hinaus so konfiguriert, dass sich der Bildschirm des mobilen Endgeräts nach spätestens 30 Sekunden sperrt, sodass das Endgerät erst nach Eingabe eines Kennworts wiederverwendet werden kann.

Darüber hinaus stellt der Verantwortliche sicher, dass der Speicher der mobilen Endgeräte verschlüsselt ist. Daten von und zu mobilen Endgeräten werden aus-schließlich verschlüsselt übertragen.

Der Verantwortliche stellt sicher, dass die Daten auf Mobiltelefonen aus der Ferne („Remote“) gelöscht werden können, wenn diese verloren gegangen sind.

Risiken:

Zugriff unberechtigter Personen, Datenverlust

Verhaltensregeln:

Es dürfen keine eigenen Endgeräte verwendet werden.

3.5. Sicherung von öffentlich zugänglichen Bereichen

Beschreibung:

Der Verantwortliche stellt kein öffentlich zugängliches WLAN für Patienten / Besucher etc. zur Verfügung. Das lokale Netzwerk ist so geschützt, dass keine fremden Personen ohne vorherige Freischaltung eingebunden werden können

3.6. Sicherung von Telekommunikationseinrichtungen

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Telekommunikationseinrichtungen (etwa Telefonanlage, Fax, VPN, W-LAN, E-Mailserver, Firewalls) vor unberechtigtem Zugriff geschützt sind.

Risiken:

Datenverlust, Zugriff von unberechtigten Personen, Hacking

3.7. Verwendung unterbrechungsfreier Stromversorgung (USV)

Beschreibung:

Server und andere Komponenten sind mit einer unterbrechungsfreien Stromversor-gung gesichert.

Risiken:

Datenverlust

3.8. Verwendung von Firewall und Virenschutz

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Systeme durch eine Firewall geschützt werden, um einen unberechtigten externen Zugriff zu verhindern. Der Verantwortliche stellt sicher, dass ein aktueller Viren- und Spamfilter installiert ist und gewartet wird.

Risiken:

unberechtigter Zugriff auf Daten, Datenverlust, Veränderung von Daten

Verhaltensregeln:

Auf Arbeitsplatzrechnern darf der Virenschutz oder die Firewall nicht durch den Nutzer deaktiviert werden.

4. Organisatorische Maßnahmen hinsichtlich IT-Infrastruktur

4.1. Dokumentation der technischen Infastruktur

Beschreibung:

Der Verantwortliche stellt sicher, dass die gesamte technische Infrastruktur ausreichend dokumentiert ist. Dies beinhaltet auch die Dokumentation und Kennzeichnung der Verkabelung sowie relevanter baulicher Maßnahmen.

4.2. Maßnahmen bei Außerbetriebnahme eines Clients / Beendigung des Dienstverhältnisses

Beschreibung:

Der Verantwortliche stellt sicher, dass sämtliche Rechner, welche nicht mehr genutzt werden sollen, ordnungsgemäß entsorgt werden und personenbezogene Daten auf den Rechnern vor unberechtigtem Zugriff geschützt werden.

Risiken:

Zugriff unberechtigter Personen

5. Organisatorische Maßnahmen bauseitig

5.1. Eingeschränkter Zutritt zum Archiv

Beschreibung:

Der Verantwortliche hat Maßnahmen dahingehend ergriffen, dass der Zutritt zum Ar-chiv nur berechtigten Personen möglich ist.

Risiken:

Zutritt von Unberechtigten

5.2. Eingeschränkter Zutritt zum Serverraum

Beschreibung:

Der Verantwortliche stellt sicher, dass Server vor unberechtigtem Zugriff geschützt (etwa versperrt) sind und eine Verfügbarkeit des Servers in ausreichendem Ausmaß sichergestellt. Schlüssel ist versperrt bei der Anmeldung. Zugriffsprotokoll ist auszufüllen.

Risiken:

Zutritt von Unberechtigten

5.3. Maßnahmen zum Schutz der Infrastruktur

Beschreibung:

Der Verantwortliche stellt sicher, dass die Infrastruktur vor unberechtigtem Zutritt geschützt ist. Ferner hat der Verantwortliche Maßnahmen ergriffen, die Infrastruktur vor Zerstörung (etwa durch Feuer) zu schützen.

Risiken:

unberechtigte Zutritte

5.4. Regelungen über das Aufrufen von Patienten und die Vertraulichkeit der persönlichen Kommunikation

Beschreibung:

Der Verantwortliche stellt sicher, dass Patienten diskret aufgerufen werden. Dazu werden der Verantwortliche oder dessen Mitarbeiter lediglich den Nachnamen des Patienten aufrufen. Der Verantwortliche und dessen Mitarbeiter werden so mit dem Patienten kommunizieren, dass ein Dritter keine Kenntnis über den Inhalt der Kommunikation erhält.

Risiken:

Mithören unberechtigter Personen

5.5. Regelungen über den Zutritt zu Räumlichkeiten

Beschreibung:

Der Verantwortliche stellt sicher, dass der Zutritt zu den Räumlichkeiten nur berech-tigten Personen möglich ist. Mitarbeiter, welche Schlüssel oder Zutrittsberechtigun-gen zu den Räumlichkeiten erhalten haben, sind entsprechend geschult, dass diese den Verantwortlichen umgehend informieren müssen, sollte der Schlüssel abhan-denkommen (Verlust, Diebstahl oder ähnliches).

Risiken:

Zutritt von Unbefugten

6. Administrative Maßnahmen

6.1. Behandlung von Sicherheitsvorfällen

Beschreibung:

Der Verantwortliche hat Prozesse definiert, was im Fall eines Sicherheitsvorfalles passieren soll.

Risiken:

Verletzung gesetzlicher Pflichten

6.2. Definition von Prozessen zu Betroffenenrechten

Beschreibung:

Der Verantwortliche hat zur Erfüllung von Betroffenenrechten Prozesse zur Auskunft, Löschung und Richtigstellung von Daten definiert und dokumentiert.

Risiken:

Verletzung gesetzlicher Pflichten

6.3. Durchführung periodischer Datenschutzaudits

Beschreibung:

Gemeinsam mit dem externen Datenschutzbeauftragten wird zumindest einmal im Jahr ein periodisches Vor-Ort Audit durchgeführt um die datenschutzrechtlichen Maßnahmen, insbesondere im Hinblick auf Datensicherheit zu auditieren. Die Ergebnisse werden in einem gemeinsamen Protokoll festgehalten und eventuelle zusätzliche Maßnahmen vereinbart.

6.4. Einsatz eines softwaregestützten Datenschutzmanagementsystems

Beschreibung:

Zur systematischen Abarbeitung und Auditierung von Datenschutzthemen wird ein softwaregestütztes Datenschutzmanagement betrieben.

Risiken:

datenschutzwidriges Organisationsverhalten

6.5. Überprüfung der Einhaltung der technischen und organisatorischen Maßnahmen

Beschreibung:

Der Verantwortliche wird regelmäßig die hier beschriebenen technischen und organi-satorischen Maßnahmen evaluieren und prüfen.

Risiken:

Verstoß gegen gesetzliche Verpflichtungen insbesondere gegen Art 32 DSGVO