Sicherheit beginnt bei Ihrem Computer

Sicherheit in der Arztpraxis

Die 10 goldenen Regeln zum Datenschutz am Computerarbeitsplatz

www.internet**sicherheitsgurt**.at

1. **Ordinationszutritt und Schutzzonen:** Der Zutritt ist nach dem heutigen Stand der Technik abzusichern und zu schützen. Lassen Sie Ihre Arztpraxis sicherheitstechnisch gegen Einbruch, Diebstahl oder Sabotage gegebenenfalls elektronisch sichern. Achten Sie darauf, dass die Schutzzonen Warte-/Patientenbereich, Verwaltungsbereich und Untersuchungsbereich strikt getrennt sind. Der Datenserver sollte in einem verschließbaren Bereich stehen.

2. **PC-Arbeitsplatz:** Verwenden Sie Hard- und Software, die dem aktuellen Stand entsprechen. Dies erhöht die Sicherheit und die Systemzuverlässigkeit. Ein aktuelles Betriebssystem mit den aktuellen Sicherheits-Updates, Passwortregelung und eine ordentliche Benutzerverwaltung gehören dazu. Regelmäßige Investitionen in Sicherheit und aktuelle Software kommen in Summe günstiger als die Folgekosten für Datenverluste.

3. **Datenschutz:** Achten Sie auf die sichere Datenspeicherung und Datenweitergabe von Patientendaten. Daten müssen Dienstleistern auf sicherem Wege zur Verfügung gestellt werden. Patientenbezogene Daten müssen daher bei der elektronischen Übertragung vertraulich und nachweisbar, also verschlüsselt und digital zu signieren sein. Papierunterlagen sind sicher zu verwahren und gegebenenfalls zu vernichten (Schreddern). Bei der Auswahl einer Firma für die elektronische Befundübermittlung sollten nur Partner gewählt werden, die nachweislich die ÖÄK-Richtlinien zur elektronischen Übermittlung erfüllen.

4. **Internet-Sicherheit, Viren, Spam und Trojaner:** Bei einer Internet-Anbindung die nicht über das GIN-Netz führt, achten Sie darauf, dass Sie eine Firewall installieren. Ein aktueller Viren- und Spamschutz ist immer einzusetzen. Öffnen Sie keine E-Mail Anhänge von unbekannten Personen, denn sie können Viren und Trojaner in Form von Schadprogrammen enthalten.

5. **Verhalten im Reparaturfall, Festplattentausch:** Lassen Sie Ihre Systeme nur von vertraglich gebundenen Fachleuten Ihres Vertrauens reparieren. Löschen Sie vor Reparatur- oder Störungsarbeiten alle Patientendaten auf sicherem Wege. Löschen oder formatieren alleine ist zu wenig, die Daten sind wieder herstellbar. Lassen Sie sich alte und/oder ausgetauschte Festplatten ggf. nach der Reparatur aushändigen.

6. **Wartung und Fernwartung:** Wartungsarbeiten sollten regelmäßig zur erhöhten Sicherheit Ihrer Daten und Systeme durchgeführt werden. Eine Fernwartung sollte von Ihnen aus angestoßen werden.

7. **Entsorgung:** Lassen Sie Ihre Computersysteme von einem Fachmann entsorgen. Machen Sie vorab eine Datensicherung (Achtung: Sie haben eine bis zu 30-jährige Aufbewahrungspflicht) und achten Sie darauf, dass die Daten auf dem zu entsorgenden Computersystem sicher gelöscht werden – ein einfaches Format-Kommando ist zu wenig.

8. **Datensicherung:** Sichern Sie regelmäßig Ihre Daten auf aktuellen Sicherheitsmedien. Vergewissern Sie sich auch durch ein probeweises Wiedereinspielen (Restore) der Daten, dass die Informationen noch lesbar sind.

9. **Geheimhaltungsvereinbarung und Dokumentation:** Schließen Sie mit Ihrem IT-Dienstleister eine Geheimhaltungsvereinbarung nach Datenschutzgesetz ab und dokumentieren Sie EDV-technische Vorkommnisse (z.B.Betrieb-automatische Protokollierung, Wartung, Störfall, Reparatur).

10. **Überprüfung der Sicherheit:** Lassen Sie Ihrer Computersysteme regelmäßig auf Sicherheit und Zuverlässigkeit überprüfen.

[1]Siehe Ärzte-, Datenschutz- und Gesundheitstelematikgesetz

ZT Prentner IT GmbH
Ziviltechnikergesellschaft für Informations- und Kommunikations-Technologie.

1010 Wien, Austria
Tel. +43 - (0)1 532 46 86-0
www.zt-prentner-it.at

ZT PRENTNER IT
STAATLICH BEFUGTER IT-ARCHITEKT