12 REGELN ZUR DATEN-SICHERHEIT

1. **RECHTLICHE VORSCHRIFTEN.** Informieren Sie sich über Ihre Rechte und Pflichten. Verschriftlichen Sie alle Vorgänge und sammeln Sie die Unterlagen an einem Ort.

2. **PHYSISCHER SCHUTZ.** Stellen Sie sicher, dass betriebsfremde Personen keine sensiblen Daten einsehen können. Beschränken und kontrollieren Sie den Zutritt, beschränken Sie absichtliche oder versehentliche Einblicke, schützen Sie die Bereiche, in denen mit sensiblen Daten gearbeitet wird. Sehen Sie einen Einbruchs- und Diebstahlschutz vor.

3. **MITARBEITER.** Weisen Sie auf die Geheimhaltungspflicht in den Dienstverträgen hin. Legen Sie in einem Schriftstück für jeden Mitarbeiter fest, welche Dateneinsicht jeder Mitarbeiter benötigt.

4. **RECHNER / BETRIEBSSYSTEM.** Benutzen Sie ein Betriebssystem, das mit Sicherheitsupdates versorgt wird, einen aktuellen Browser sowie einen aktuellen Virenschutz. Überprüfen Sie Ihre Rechner unter www.peeringpoint.at/browsersicherheit. Falls Sie auf das Internet ohne GIN (e-card-Netzwerk) zugreifen, aktivieren Sie eine Software-Firewall.

5. **ORDINATIONSSOFTWARE.** Überprüfen Sie, ob eine Mitarbeiterverwaltung mit persönlichem Login unterstützt wird, fordern Sie eine starke Passwortqualität. Beschränken Sie die Zugriffe Ihrer Mitarbeiter auf die notwendigen Daten und stellen Sie sicher, dass die tatsächlichen Datenzugriffe protokolliert werden.

6. **DATENSICHERUNG.** Sichern Sie regelmäßig alle wesentlichen Daten Ihres IT-Systems. Bewahren Sie die Sicherungsmedien extern oder an einem geschützten Ort (Safe) auf. Kontrollieren Sie periodisch die Qualität der Medien und prüfen Sie die Wiederherstellbarkeit Ihres Systems. Treffen Sie Vorkehrungen für einen Softwarewechsel oder die Beendigung Ihrer ärztlichen Tätigkeit.

7. **DATEN ÜBERTRAGEN.** Übertragen Sie personenbezogene Daten nur mit gesicherter Befundübertragung oder (unter den gesetzlich vorgesehenen Auflagen) per Fax. Verwenden Sie keinesfalls E-Mail!

8. **DIENSTLEISTERVERTRÄGE.** Stellen Sie die Geheimhaltungsverpflichtung schriftlich sicher. Regeln Sie die Möglichkeiten der Fernwartung und den Zugriff auf Daten oder Sicherungsmedien. Erfragen Sie in Ihrer Ärztekammer die entsprechenden Vorlagen. Vermeiden Sie unbeschränkte Fernwartungszugänge.

9. **REPARATUR/ENTSORGUNG.** Geben Sie Datenträger nur ohne Daten an Dritte weiter, zerstören Sie gegebenfalls selbst die Festplatten. Denken Sie an den Inhalt von Sicherungsmedien. Fordern Sie von dem Dienstleister eine schriftliche Bestätigung der Einhaltung des Datenschutzes.

10. **PERSÖNLICHES VERHALTEN.** Gehen Sie mit den neuen Medien und Möglichkeiten kritisch um: Öffnen Sie keine E-Mails von unbekannten Personen, misstrauen Sie Gratisversprechungen, geben Sie keine vertraulichen Daten bekannt – so wird beispielsweise keine Bank oder Kreditkartenfirma Informationen von Ihnen per E-Mail einholen!

11. **NEUE GEFAHREN BEDENKEN.** Sichern Sie ein verwendetes WLAN nach dem Stand der Technik ab. Denken Sie an Daten auf mobilen Geräten (Notebook, Tablet, Smartphone), insbesondere bei Weitergabe und Diebstahl. Externe Zugriffe auf die Ordinationsdaten sind entsprechend zu sichern.

12. **REGELMÄSSIGE ÜBERPRÜFUNGEN.** Die aktuelle Technik und die damit verbundenen Möglichkeiten und Gefahren schreiten rasant voran. Denken Sie bei allen Konfigurationsänderungen auch an die IT-Sicherheit und dokumentieren Sie alle wesentlichen Vorgänge. Aktualisieren Sie in regelmäßigen Abständen Ihr IT-Sicherheitskonzept.

Eine Empfehlung von

BUNDESKURIE NIEDERGELASSENE ÄRZTE

ÖSTERREICHISCHE ÄRZTEKAMMER