

S&N Datentechnik Checkliste bei elektronischer Patientendatenverwaltung

- ✓ Unbefugten ist der Zutritt zu Datenverarbeitungseinrichtungen (PC-Hardware), mit denen Patientendaten verarbeitet werden, zu verwehren.
- ✓ Es ist zu verhindern, dass Datenverarbeitungssysteme (Software) von Unbefugten genutzt werden können.
- ✓ Es ist zu gewährleisten, dass Patientendaten bei der elektronischen Übertragung, ihrem Transport oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
- ✓ Es ist zu gewährleisten, dass Patientendaten gegen zufällige Zerstörung oder Verlust geschützt sind.
- ✓ Passwörter für das Datenverarbeitungsprogramm sollten zur Sicherheit bestimmten Anforderungen genügen, um sich vor Hackerwerkzeugen zu schützen.
- ✓ Passwörter sollten immer mehr als 7 Zeichen umfassen, nicht in Wörterbüchern vorkommen sowie nicht aus Namen und persönlichen Geburtsdaten bestehen. Ferner empfiehlt es sich, Sonderzeichen wie z.B.: &, \$, %, * mitzubedenken.
- ✓ Passwörter müssen umgehend verändert werden, sobald der begründete Verdacht besteht, dass jemand unbefugt Zutritt am PC hatte!
- ✓ Passwörter und Konfigurationen für Fernzugriff sollten niemals niedergeschrieben werden!
- ✓ Aktuelle Virenschutzprogramme sind auf den in der Praxis genutzten Rechnern unverzichtbar.
- ✓ E-Mails mit nicht vertrauenswürdigen Anhängen im Anhang, wie z.B. 7-Zip-Rechnungen, Word-Dateien, Excel-Tabellen usw. nicht öffnen! Im Zweifelsfall die S&N Datentechnik anrufen!
- ✓ Immer abmelden: z.B. Online-Banking, E-Mail Portale usw.