IT Sicherheit in den Ordinationen	BUNDESKURIE NIEDERGELASSENE ÄRZTE
4. Serienteil: Die Arztsoftware und IT Sicherheit	

Arztsoftware und IT Sicherheit

Ohne Arztsoftware ist das Verwalten einer Ordination kaum noch möglich. Damit Sie von den Vorteilen moderner EDV profitieren können und gleichzeitig rechtlich abgesichert sind, sollten Sie eine Reihe von Grundregeln einhalten. Unsere Info-Serie der Kurie Niedergelassene Ärzte zeigt Ihnen, worauf es dabei ankommt.

Eine Serie von DI Michael Nöhammer

In so gut wie jeder Ordination – zumindest im Vertragsarztbereich – wird heute eine Arztsoftware eingesetzt. Diese dient hauptsächlich zur administrativen Verwaltung der Ordination, in noch relativ wenigen Fällen unterstützt die Software auch die medizinische Arbeit. Aus Sicht der IT-Sicherheit stehen im Folgenden nicht die benötigten Funktionalitäten im Vordergrund, sondern der sichere Umgang mit sensiblen Daten.

Wer darf was?

Aus Sicht des Datenschutzes ist es wichtig, „die Zugriffsberechtigung auf Daten und Programme und den Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln“ (Datenschutz-Gesetz 2000). In Bezug auf den Einsatz von Arztsoftware bedeutet das, dass es für jeden Mitarbeiter einer Ordination genau geregelt sein muss, auf welche Daten und Programm er zugreifen darf. Diese Regelung sollte bereits im Rahmen des Dienstvertrages festgeschrieben sein.

Erforderlich ist selbstverständlich ein „personalisiertes Login“, das auch konsequent verwendet werden muss: Jeder Benutzer hat sich sich mit einem persönlichen Kennwort der Arztsoftware gegenüber zu identifizieren, nur so kann die Arztsoftware die Berechtigungen der einzelnen Benutzer verwalten und den Zugriff freigeben. Auf eine ausreichende Passwortqualität (Länge, Klein-/Großbuchstaben, Ziffern, Sonderzeichen) ist zu achten.

Dokumentation für den Ernstfall

Außerdem ist von der Arztsoftware Protokoll über die tatsächlich durchgeführten Verwendungsvorgänge zu führen. Es muss für den Datenverantwortlichen (i.d.R. der Inhaber der Ordination) jederzeit ersichtlich sein, welcher Mitarbeiter auf welche Weise (lesen, schreiben, ändern) auf welche Daten zugegriffen hat. Diese Dokumentation ist vor allem bei mutmaßlichen Verletzungen des Datenschutzes von Bedeutung, weil bei einem Gerichtsverfahren derartige Aufzeichnungen als Beweise vorgelegt werden müssen.

Üblicherweise werden auch Daten wie Befunde, Abrechnungen, etc., die in der Arztsoftware gehalten werden, an andere Teilnehmer im Gesundheitswesen übertragen („exportiert“). Diese Vorgänge werden in einem eigenen Artikel dieser Serie betrachtet, hier geht es nur um die Arztsoftware selbst.

Datenzugriff von außen

Durch den Fortschritt der Technik ist es vielfach bereits möglich, dass auf die Arztsoftware von außerhalb zugegriffen wird. Das ist z. B. im Falle einer Zweitordination oder für Arbeiten im privaten Umfeld sehr praktisch, auch die Betreuer der Arztsoftware greifen oftmalig per

Fernwartung auf diese zu. Der Zugriff ordinationsfremder Personen (Hard- und Softwarebetreuung, EDV-Dienstleister, …) ist jedenfalls vertraglich zu regeln, Dritte müssen schriftlich die Einhaltung des Datenschutzes garantieren. Für alle Fernzugriffe ist die technische Sicherheit, der Schutz vor unbefugtem Zugriff, zu garantieren, alle Maßnahmen sind zu dokumentieren.

Stellen Sie sich vor …

Sie kommen Montagfrüh in Ihre Ordination, ein arbeitsreicher Tag erwartet Sie. Sie versuchen, Ihre EDV einzuschalten – leider ohne Erfolg. Der Server startet nicht, Sie haben keinen Zugriff auf Ihre Daten.

Was tun Sie? Zusperren? Patienten ohne Daten behandeln? Alles manuell schreiben und nachtragen? Wie geht das dann mit der ecard, wer hilft Ihnen?

Bereiten Sie also am besten möglichst bald für solche Fälle einen Notfallplan vor:

- Wo können Sie Ersatz-Hardware organisieren?
- Gibt es Garantien, Wartungsverträge?
- Wer installiert die Software auf der neuen Hardware?
- Ist der IT Dienstleister schnell genug verfügbar?
- Sind Passwörter, Codes, Lizenzen verfügbar?
- Haben Sie die Notrufnummern ihrer Dienstleister?
- Wurden Reaktionszeiten vertraglich geregelt?

Für jede Ordination sind die Daten in der Arztsoftware als äußerst wichtig einzustufen, meistens ist eine Arbeit ohne Arztsoftware kaum noch vorstellbar. Daher ist die Sicherung dieser Daten die wichtigste Maßnahme, die jeden Tag durchgeführt werden muss. Die Datensicherung besteht im Wesentlichen in einer Kopie der Daten auf externen Medien (z.B. Festplatte, Band, USB-Stick), wobei Sie folgende Punkte sicherstellen müssen:

- Sichern Sie alle Daten, die für einen reibungslosen Betrieb notwendig sind, auch Konfigurationsdateien, Zusatzprogramme für EKG, Medizintechnik, Mail und notwendige Software und wichtige Daten auf den Stationen
- Prüfen Sie die Korrektheit der Sicherung. Kann man alle Daten aus der Sicherung wiederherstellen, ist Ihr System nach einer Wiederherstellung vollständig benutzbar?
- Sollten Sie dies nicht selbst durchführen können, beauftragen Sie Ihren IT-Dienstleister damit und lassen Sie sich das Ergebnis schriftlich bestätigen – damit haftet der Dienstleister auch für die Korrektheit der Sicherung.
- Sollten der Arztsoftwarehersteller und der IT-Dienstleister unterschiedliche Firmen sein, legen Sie eine eindeutige Verantwortung für Sicherung und Wiederherstellung fest.

Verwehren Sie Unbefugten den Zugriff auf die Sicherungen. Dies kann durch Datenverschlüsselung oder durch sichere physische Verwahrung (Safe) geschehen. Verteilen Sie die Sicherung auf mehrere Orte. Nach einem Brand oder Wasserschaden können alle in der Ordination gelagerten Sicherungskopien unbrauchbar sein.

Praxistipps	
√	Stellen Sie sicher, dass Ihre Arztsoftware dem Datenschutzgesetz entspricht.
√	Sichern Sie Ihre Daten und überprüfen Sie die Wiederherstellbarkeit.