Die rechtlichen Grundlagen der Arbeit mit Datensicherheit

Was ist Datenverarbeitung? Welche Informationen dürfen in welcher Form weitergegeben werden? Was verlangt der Gesetzgeber von Ärztinnen und Ärzten? Die Bundeskurie niedergelassene Ärzte informiert Sie in einer Artikelserie über die wichtigsten Fragen zum Thema Informationstechnik und Datenschutz: Damit Sie auf der sicheren Seite sind.

Dr. Jutta Adlbrecht

Die gesetzlichen Vorschriften zum Thema Datenschutz finden sich im Datenschutzgesetz (DSG 2000) 2000 und im Gesundheitstelematikgesetz (GTelG): Das DSG regelt allgemein die Verwendung von Daten, das GTelG normiert im Speziellen die Weitergabe von sensiblen Daten. Für die Tätigkeit in Ordinationen ist aufgrund der Verwendung von Gesundheitsdaten, welche als „sensible personenbezogene Daten" zu qualifizieren sind, sind sowohl das DSG 2000 als auch das GTelG anzuwenden.

Datenverarbeitung und Datenübermittlung

Gemäß dem Ärztegesetz (ÄrzteG) sowie dem Krankenanstalten- und Kuranstaltengesetz (KAKuG) ist jede Ärztin und jeder Arzt verpflichtet, beratende, diagnostische oder therapeutische Leistungen zu dokumentieren. Diese Dokumentation ist rechtlich sogenannte „Datenverwendung" zu verstehen: Dieser Begriff beinhaltet die „Datenverarbeitung" innerhalb einer Ordination und die „Datenübermittlung", also die Übertragung von Daten von bzw. nach außen.

Die Datenverwendung von personenbezogenen Daten ist innerhalb einer Ordination zulässig, sofern sie dem Zweck der medizinischen Behandlung oder der Abrechnung mit der Sozialversicherung dient. Das DSG 2000 zählt noch einige Fälle auch, bei denen eine Datenverwendung zulässig ist, z.B. medizinische Forschung. Sollen personenbezogene Daten jedoch für andere Zwecke verarbeitet oder übermittelt werden, ist das Einverständnis der betroffenen Person einzuholen.

Für „nicht personenbezogene Daten", also anonyme Daten, gelten diese Einschränkungen nicht. Solche Daten können ohne weiteres vom Dateninhaber, also der Ärztin oder dem Arzt, weitergegeben werden.

In einer Ordination ist die Ärztin oder der Arzt datenschutzrechtlich als „Auftraggeber" der Datenverwendung zu betrachten. Der Auftraggeber ist für die Datenverwendung verantwortlich, kann sich jedoch zur Unterstützung etwaiger „Dienstleister" bedienen. Diesfalls sollte sich der Auftraggeber die datenschutzkonforme Abwicklung der Dienstleistung schriftlich zusichern lassen.

Wozu Ärzte per Gesetz verpflichtet sind

Die einschlägigen Gesetze verpflichten Ärztinnen und Ärzte zum Ergreifen von Maßnahmen zur Gewährleistung der Datensicherheit.

Dabei ist sicherzustellen,

- dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind,
- dass ihre Verwendung ordnungsgemäß erfolgt,
- dass die Daten Unbefugten nicht zugänglich sind.

All das unter Berücksichtigung des Standes der technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit.

Erforderliche Maßnahmen

Was bedeutet das konkret? Das DSG 2000 zählt beispielhaft einige erforderliche Maßnahmen auf, es obliegt aber der Verantwortung jeder Ärztin und jedes Arztes, weitere notwendige Maßnahmen zu treffen, die der Datensicherheit dienen.

Als grundsätzlich wichtige Maßnahmen gelten:

- die Aufgabenverteilung zwischen allen Beteiligten (Ärztinnen, Ärzten, Mitarbeiterinnen, Mitarbeitern) festzulegen, diese schriftlich festzuhalten und die Verwendung von Daten an ebenfalls schriftliche Aufträge zu koppeln;
- alle Beteiligte schriftlich über die Datenschutzvorschriften zu belehren;
- die Zutrittsberechtigung zu den Räumlichkeiten der Ordination zu regeln;
- die Zugriffsberechtigung auf Daten und Programme festzulegen. Dazu gehört ein personengebundenes Login in alle verwendeten Softwareprodukte;
- Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge nachvollzogen werden können: insbesondere Änderungen, Abfragen und Übermittlungen;
- über alle Maßnahmen eine Dokumentation zu führen. Diese ist wesentlicher Bestandteil eines „IT Sicherheitskonzeptes".

Direkt abgeleitet aus den gesetzlichen Verpflichtungen können insbesondere folgende Maßnahmen werden:

- Die Sicherung vor Verlust und Zerstörung (Hardware-Gebrechen, Sabotage, Fehleingaben, etc.) und Vorkehrungen gegen zufällige Ereignisse (Stromausfall, Wasserschaden, Feuer, etc.). Als wesentliche Maßnahme kann eine Datensicherung durchgeführt werden.
- Die Erfüllung der Informations- und Auskunftspflicht gegenüber Patientinnen und Patienten. Damit ist die Sicherstellung eines reibungslosen und dauerhaften Betriebs der IT in der Ordination gemeint. Beachten Sie auch die Auskunftspflichten nach Beendigung der Ordinationstätigkeit.

Praxistipps	
√	Wenden Sie die gesetzlichen Vorschriften praxisgerecht in Ihrer Ordination an
√	Verschriftlichen Sie alle Vorgänge
√	Erstellen Sie ein IT Sicherheitskonzept – siehe dazu Serienteil 8